Nebraska Law Review

Volume 82 | Issue 3 Article 5

2004

Commercial Use of Protected Health Information Under HIPAA's Privacy Rule: Reasonable Disclosure or Disguised Marketing?

June Mary Makdisi
St. Thomas University, jmmakdisi@stu.edu

June Mary Zekan Makdisi*

Commercial Use of Protected Health Information Under HIPAA's Privacy Rule: Reasonable Disclosure or Disguised Marketing?

TABLE OF CONTENTS

* Associate Professor of Law, St. Thomas University College of Law; B.A., University of Pennsylvania; M.S., University of Pennsylvania; J.D., University of Tulsa College of Law.

I. INTRODUCTION

April 14, 2003 marked the beginning of a new era in America's healthcare industry. Gone are the days of unlimited access to patient health care information by members of the heath care professional community. Instead, as of April 14, 2003,[1] access or exchange of the sensitive data may occur only under the conditions outlined in a complex new regulatory scheme referred to as the Privacy Rule.[2] The Rule, meant to safeguard health information privacy, is an offshoot of health care directives provided by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[3]

This Article explores how well the Rule protects patient privacy, particularly in the context of permissible disclosures that a consumer might regard as commercial marketing. Part I introduces the issue by explaining the implementation of the initial Privacy Rule and its modified version under HIPAA. Part II briefly familiarizes the reader with the complexity of defining privacy and establishes which definition to use in analyzing the Rule. Part III evaluates the Rule as a whole, determining whether the move from consent in the initial Rule to mere notice about information disclosures in the modified Rule adequately protects privacy. This Article then highlights the effectiveness of the Rule's notice requirements in connection with disclosures under three types of circumstances – treatment, payment, and health care operations. Deciphering the last category reveals the serious infractions created by the ability to mask commercial marketing under the guise of health care operations. Part IV summarizes the major concerns and provides practical solutions to shore up patient privacy.

II. NEED FOR A PRIVACY RULE

Congressional intent in enacting HIPAA was to ensure continued health insurance coverage for those who changed jobs or insurance

1. 45 C.F.R. § 164.534 (2001) (the "Rule" or the "Privacy Rule") (the regulations provide an additional year's grace for small health plans).
2. *Id.* at §§ 164.500 to 164.534 (Standards for Privacy of Individually Identifiable Health Information). A companion set of regulations (the Security Rule) dictates in greater detail how entities are to maintain the security of the information they will hold and transmit. *See* 45 C.F.R. §§ 164.302 to 164.318 (2003). Many workshops, for example, have been and will be offered to prepare industry, and their attorneys for the changes brought about by the Rule. *E.g.*, "HIPAA for Real People - the Series" (5 part series presented in early 2003 by the ABA Health Law Section, in conjunction with others) *at* www.abanet.org/health/ (2003).
3. Health Ins. Portability and Accountabiliy Act of 1996 (HIPPA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (also known as the Kassebaum-Kennedy Act) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.A.).

policies[4] and to reduce "waste, fraud and abuse in health insurance and health care delivery."[5] A driving force of the Act was to reduce cost and increase efficiency within the health care system, at least as it related to billing[6] and maintaining health insurance coverage, meant to safeguard health privacy as electronic storage and transmission of the information has increased the nation's vulnerability to exposure.

Implementation of the statutory purpose was to be accomplished by means of an "Administrative Simplification" of records requiring a computerized infrastructure to maintain and transmit records electronically. Of necessity, a unique health care identifier would need to link the amassed health care information with the individual who was the subject of the information.[7] The need, really, the requirement, that information pass quickly between agencies via the digitized networks of electronic storage and transmission meant an increased exposure to unauthorized access to the information with a resultant increased need for privacy protection.[8] The industry was already plagued by scandalous leaks that had seriously undermined the public's trust.[9] Further exposure necessitated protective action to win the

4. Scott J. Kelly, *The Health Insurance Portability and Accountability Act of 1996: Medicare Fraud Advisory Opinion Mandate Sends the Inspector General " Shopping for Hats,"* 59 OHIO ST. L.J. 303, 316 (1998).

5. HIPAA (Preamble), 110 Stat. 1936 [hereinafter Preamble].

6. HIPAA, 110 Stat. 1936; *See also* 42 U.S.C. § 1320d-2 (Supp. 1999) ("encouraging use of electronic medical records"); HIPAA, 110 Stat. 2033, § 264(a) (1996) ("requiring promulgation of regulations of 'standards with respect to the privacy of individually identifiable health information' by the Department of Health and Human Services if Congress did not act"); Henry T. Greely, *Trusted Systems and Medical Records: Lowering Expectations*, 52 STAN. L. REV. 1585, 1587-88 (2000).

7. Eric Wymore, *It's 1998, Do You Know Where Your Medical Records Are? Medical Record Privacy After the Implementation of the Health Insurance Portability and Accountability Act of 1996*, 19 HAMLINE J. PUB. L. & POL'Y 553, 566-568 (1998); 42 U.S.C. § 1320d-8 (1998); 42 U.S.C. § 1320d-2(a), (d) (1998) (requiring the Secretary of the Dept. of Health and Human Services to promulgate security standards to protect health information).

8. *See* Lawrence O. Gostin, et al., *Balancing Communal Goods and Personal Privacy Under a National Health Informational Privacy Rule*, 46 ST. LOUIS U. L.J. 5, 6 (2002); *see also* Rob Reilly, *Conceptual Foundations of Privacy: Looking Backward Before Stepping* Forward, 6 RICH. J.L. & TECH. 6, *3 (1999).

9. *See, e.g.*, Paul Starr, *Health and the Right to Privacy*, 25 AM. J.L. & MED. 193, 197 (1999); Standards for Privacy of Individually Identifiable Health Information [hereinafter Preamble], *at* http://www.aspe.hhs.gov/admnsimp/final/PvcPre01.htm (2000).

trust and resultant cooperation of the public.[10] Thus, protecting individual privacy became a secondary "other purpose" of the Act.[11]

The recognition that increased privacy protection is needed in a digital world is hardly unique to the United States. Worldwide, most view privacy in general as a basic human right.[12] To safeguard the right of privacy, many countries have adopted generic legislation that protects all forms of privacy. The United States, by contrast, takes a piecemeal approach.[13] In accord with a perceived need for the protection of personal health information, Congress mandated that specifics be hammered out either in Congress directly, or, in the event that no consensus could be reached in enacting companion legislation, through agency rulemaking.[14]

Despite several bills, Congress failed to enact personal health privacy legislation. Some have suggested that conservative camps, associated with industry more than with plaintiffs whose personal information would be the subject of the legislative efforts, stymied the progress. Political conservatives have been accused of employing rhetoric to achieve the desired result of squashing legislation, arguing somewhat opposite positions that current protections are adequate and also that suggested language was both "too broad" and "without

10. *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Information,* 76 TEX. L. REV. 1, 69-70 (1997); Standards for Privacy of Individually Identifiable Health Information (preamble), http://www.aspe.hhs.gov/admnsimp/final/PvcPre01.htm (2002) ("Unless public fears are allayed, we will be unable to obtain the full benefits of electronic technologies.") ("administrative simplification cannot succeed if we do not also protect the privacy and confidentiality of personal health information").

11. A. Craig Eddy, *Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of the Health Insurance Privacy and Accountability Act of 1996,* 9 ANNALS HEALTH L. 1, 17 (2000).

12. David Banisar, *Privacy and Human Rights 2000, at* http://www.privacyinternational.org/survey/phr2000 (last visited April 22, 2002); *see also* James D. Molenaar, *The HIPAA Privacy Rule: It Helps Direct Marketers Who Help Themselves to Your Personal Health Information,* 2002 L. REV. MICH. ST. U. DET C.L. 855 (2002) (demonstrating privacy is a fundamental right in the United States as well).

13. John D. Blum, *The Role of Law in Global E-Health: A Tool for Development and Equity in a Digitally Divided World,* 46 ST. LOUIS U. L.J. 85, 97 (2002). For an example of some legislative efforts, see Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy,* STAN. L. REV. 1393, 1440-44 (2001). *See also* Gostin, *supra* note 8, at 13-14 (describing various privacy statutes); and Lawrence O. Gostin, et al., *The Nationalization of Health Information Privacy Protections,* 37 TORT & INS. L.J. 1113, 1121-1122 (2002) (describing their weaknesses).

14. *See* 42 U.S.C. § 1320d-2 (1999); Bartley L. Barefoot, *Enacting a Health Information Confidentiality Law: Can Congress Beat the Deadline?* 77 N.C. L. REV. 283, 315-16 (1998).

new 'real' protections."[15] Upon the passing of the requisite time without effective Congressional action, the responsibility for promulgating the appropriate rules automatically fell to the Department of Health and Human Services (HHS) to complete the Congressional work.[16]

The final rules promulgated by the HHS fall within the Administrative Data Standards and Related Requirements subchapter,[17] and include regulations specifically related to privacy.[18] The regulations apply to defined "covered entities," which include health plans, health care clearinghouses, and health care providers who transmit health information electronically.[19] Of particular concern is the individually identifiable health information, termed "protected health information," or PHI.[20] The preamble to the regulations discusses privacy issues at length. To what extent does the Rule protect individual privacy? Is the protection adequate or even a primary objective of the Rule?[21] The Rule has been given mixed reviews, from offering the most advanced to the most anti-privacy protections in years.[22]

Close examination of the regulatory provisions suggests that the Rule likely affords adequate protection in the context of treatment and payment. By contrast, the Rule inadequately protects individual privacy under the rubric of health care operations.[23] Within that struc-

15. Richard S. Fedder, *To Know or Not to Know: Legal Perspectives on Genetic Privacy and Disclosure of an Individual's Genetic Profile,* 21 J. LEGAL. MED. 557, 558-59 (2000). Conservatives are thought to be aligned with defense interests and defense interests have "potent influence on judicial outcomes." (More so than plaintiff-friendly lobbying efforts). *See* Ray B. Flemming, *Contested Terrains and Regime Politics: Thinking About America's Trial Courts and Institutional Change*, 23 L. & SOC. INQUIRY 941, 959 (1998); Anita Bernstein, *The New-Tort Centrifuge,* 49 DEPAUL L. REV. 413, 424 (1999), (citing Ralph Nader, *Lawyers and Law Students as Tools of Democracy*, 17 WHITTIER L. REV. 3, 5 (1995)).
16. HIPAA § 264(c)(1), 42 U.S.C. § 1320d-2 n.2.
17. 45 C.F.R. Parts 160-164 (2001).
18. 45 CFR §§ 164.102-164.534 (2001).
19. *Id.* at § 164.104. Groups such as life insurers and workers' compensation insurers are not entities governed by the Rule. Gostin, et al., *supra* note 13, at 1126.
20. 45 C.F.R. § 164.501 (defining PHI). In addition, e-commerce sites that sell products or offer health advice may not fall within the regulatory framework. Nicholas Terry, *Regulating Health Information: A US Perspective,* 324 BRIT. MED. J. 602, 604 (2002), *available at* http://www.bmj.com.
21. *See* Preamble, *supra* note 9 ("Unless public fears are allayed, we will be unable to obtain the full benefits of electronic technologies.") ("administrative simplification cannot succeed if we do not also protect the privacy and confidentiality of personal health information"). This suggests that the primary purpose is not privacy at all, but merely the illusion of privacy in order to acquire the public's trust so that the efficiency objectives of the Rule could be achieved.
22. Charity Scott, *Is Too Much Privacy Bad for Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy,* 17 GA. ST. U. L. REV. 481, 511-12 (2000) (quoting Health Privacy Project director Janlori Goldman, privacy advocate Robert Gellman, and the ACLU).
23. Scott, *supra* note 22, at 511 (citing the Health Privacy Project and describing loopholes in the marketing provisions).

ture, many transactions that lay consumers would consider marketing are hidden under the complexities of "health care operations." Descriptions of disclosure practices contained within the entity notice are unlikely to render consumers fully aware of the purposes sanctioned by the Rule or of the extent to which their private information is disseminated. This, coupled with an inability to control the process, strongly suggests that the Rule, in the context of this disguised marketing, inadequately protects privacy.

The Rule underwent several transformations during the administrative process that lead to its initial publication as a Final Rule.[24] Then, the initial Final Rule morphed again.[25] The discussion that follows examines both the initial and the later versions of the Final Rule and demonstrates that the latter version not only fails to cure, it further erodes privacy.

III. PRIVACY DEFINED

Privacy cannot be summed up in a single definition.[26] The word "privacy" could refer to the right to make intimate decisions, the right to limit or be free from access to one another, or the right to maintain secrecy.[27] The autonomous decision-making aspect of privacy is best understood by reference to the series of reproductive liberty cases beginning with *Griswold v. Connecticut*.[28] The second aspect of privacy is perhaps best reflected in the intrusion upon seclusion privacy tort. The foundation for the tort is the right to be "let alone,"[29] which grants each person a right to exclude others from some physical or

24. 67 Fed. Reg. 53182-01 (2002) (outlining the historical progression).

25. *See* 67 Fed. Reg. 53182-01 (2002) (noting that the Final Rule was modified on August 14, 2002, with the effective date of the modifications as Oct. 15, 2002). In between the initial and modified version were the proposed changes, some of which were adopted by the modified version of the Rule. *See* INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY, GEORGETOWN UNIVERSITY, HEALTH PRIVACY PROJECT, COMMENTS ON PROPOSED MODIFICATIONS TO FEDERAL STANDARDS FOR PRIVACY ON INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (2002), *available at* http://www.healthprivacy.org/usr_doc/NPRM_HPPComments.pdf. (2002) (commenting on the proposed changes to the Rule).

26. *See generally*, LAWRENCE O. GOSTIN, PUBLIC HEALTH LAW: POWER, DUTY, RESTRAINT 127-142 (2000) (describing types of privacy, the development of trust, and fair information practices).

27. JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 56 (1992); *see also* Jean L. Cohen, *Is Privacy a Legal Duty? Reconsidering Private Right and Public Virtue in the Domain of Intimacy, in* PUBLIC AND PRIVATE: LEGAL, POLITICAL AND PHILOSOPHICAL PERSPECTIVES 117, 133-34 (Maurizio Passerin d'Entreves & Ursula Vogel eds. 2000) (describing where privacy acknowledges self-defined boundaries with respect to physical self and communications about personal matters).

28. 381 U.S. 479 (1965).

29. THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 1-7, 20 (2d ed. 1888).

mental space considered personal under the law.[30] A variety of activities impacted by the intrusion tort include eavesdropping, spying, prying, and harassment.[31] Another aspect of privacy concerns maintaining control over the flow of information about oneself.[32]

Not all loss of control impacts privacy because not all information about oneself may be considered "private." It is the information itself that gives structure to what is or is not private.[33] If the information is content neutral, then the desire to thwart its dissemination merely falls within the category of secrecy. Secrecy does not impact privacy unless the information is also intimate.[34] Information about one's health is considered "intimate."[35] Thus, failure to keep secret, or maintain the confidentiality of, health information, thereby impacts individual privacy.

The privacy regulations focus on the latter aspect of privacy – that of maintaining the secrecy of individuals' health information. In the context of medical treatment, an individual must share intimate information concerning aspects of his or her health with another who provides the treatment. Privacy is achieved by keeping this information confidential – that is, by ensuring that further disclosure is withheld unless for desired purposes.[36]

IV. Privacy in an Integrated Health Care System Envisioned by HIPAA

What are the proper and desirable purposes for which disclosure may occur without impacting privacy? A sense of privacy correlates with autonomy.[37] So in a large sense, the answer is in the subjective

30. June Mary Z. Makdisi, *Genetic Privacy: New Intrusion a New Tort?* 34 CREIGHTON L. REV. 965, 988-89 (2001).

31. *Id.* at 985-86.

32. *See* Mark A. Rothstein, *Genetic Privacy and Confidentiality: Why They Are So Hard to Protect*, 26 J. L. MED. & ETHICS 198 (1998); A.L. Allen, *Genetic Privacy: Emerging Concepts and Values, in* GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 31-59 (Mark A. Rothstein ed., 1997).

33. INNESS, *supra* note 27, at 57-59.

34. *See Id.*

35. Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing under the National Health Information Privacy Rule*, 86 MINN. L. Rev. 1439, 1440 (2002); Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L. J. 1085, 1149 (2002) (quoting Robert R. Blair, *Redefining Information Privacy*, PRIVACY J. 7 (1989)).

36. *See* Solove, *supra* note 13, at 1439; *see also* Lucas D. Introna, *Privacy and the Computer: Why We Need Privacy in the Information Society, in* CYBERETHICS: SOCIAL AND MORAL ISSUES IN THE COMPUTER AGE 195 (Robert M. Baird et al. eds, 2000).

37. *See* Carol M. Bast, *What's Bugging You? Inconsistencies and Irrationalities of the Law of Eavesdropping*, 47 DEPAUL L. REV. 837, 900 (1998).

view of the autonomous individual.[38] The individual could control the information flow through informed consent, which is the prevailing practice regarding health care in general,[39] with the extent of information shared regulated by the degree to which the individual desires to participate in society.[40] In this case, the defined society is the organized health care system. Individualized control would mean that the individual could determine what and how information was shared in exchange for participation in the system. The *quid pro quo* would be the individual's receipt of some benefit, in this case, health care. The advantage of this type of "negotiated disclosure,"[41] which is akin to a private agreement between the individual and the entity receiving the individual's information, is that by granting or withholding consent, the individual acts as a true and voluntary participant in the system.[42]

In the initial final rule, the regulatory structure required the individual's consent before entities included within the Rule's purview could use[43] or disclose[44] the individual's protected health information for purposes of treatment, payment, or health care operations.[45] Some considered this requirement of consent highly important in providing privacy protection in disclosure-centric frameworks such as this.[46] The Rule also had a "plain language" and informational requirement. This necessitated formulating a consent form that informed individuals about several rights. Among these, the right to review the entity's notice before signing the consent form[47] permitted the individual to gain insight into the entity's disclosure practices in each of the three categories.

This format appears to be a "negotiated disclosure." That is, when an individual executes a consent form, it evidences a private agreement between the participant and the entity. Use and disclosure of the private information is exchanged for health care services in accord

38. *See* RUTH R. FADEN ET AL., A HISTORY AND THEORY OF INFORMED CONSENT 259-61 (1986).
39. Gostin & Hodge, *supra* note 35, at 1467.
40. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).
41. *See* Fedder, *supra* note 15, at 570.
42. *See id.*
43. A "use" refers to the sharing of PHI within an entity. 45 C.F.R. § 164.501.
44. "Disclosure" refers to information passed on to anyone outside the particular entity holding the information. *Id.*
45. 45 C.F.R. § 164.506(a) (2001). Those subject to the Privacy Rule are health plans, health care clearinghouses, and health care providers who transmit health care information electronically in connection with a transaction covered by the Rule. 45 C.F.R. § 160.102(a) (2001). The modified Rule left this provision unchanged. *See* 45 C.F.R. § 160.103 (defining "covered entity") (2002).
46. *See* Terry, *supra* note 20, at 604.
47. 45 C.F.R. § 164.506(c) (2001). The "plain language" requirement continues in the modified version. 45 C.F.R. § 164.506 (2002).

with the entity's notice.[48] If both parties exercise free choice in entering the arrangement, the Rule protects the individual's privacy because each individual appears to maintain control over the dissemination of the private information.[49] Closer examination of any consent limitations is warranted to determine the existence of negotiated disclosure in reality or merely in appearance.

A. Limitations to Consent

One limitation to the effectiveness of the consent provision under the initial final rule was evidenced by the way in which uses and disclosures could occur in the absence of prior consent.[50] For example, health care providers who fit within the Rule's definition of "indirect treatment relationship"[51] had no need to obtain consent prior to use or disclosure.[52] An illustration helps explain the significance of the distinction between direct and indirect providers.

Suppose an individual visits his or her physician. The doctor refers the individual to another provider,[53] who withdraws blood and performs whatever tests were ordered by the initiating physician. The latter reports the findings to the initiating physician. Based on the results, the physician phones in a prescription to the pharmacy selected by the individual. The individual picks up the medication and goes home.

As a direct provider, the initiating physician would have been bound by the prior consent rules and would have been limited in his or her use or disclosure of the individual's protected health information without it. If either the testing provider or the pharmacist were considered a direct provider, then the same rules governing the initiating physician's conduct would apply to each. If, on the other hand, either were considered health care providers who delivered treatment only indirectly, then no consent would have been needed prior to use or

48. *See* Fedder, *supra* note 15, at 570.

49. *See* INNESS, *supra* note 27, at 57; *see also* Rothstein, *supra* note 32.

50. 45 C.F.R. § 164.506(a)(2)-(4) (2001).

51. 45 C.F.R. § 164.501 (2001) (providing the following definition of indirect treatment relationship: "(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and (2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual").

52. 45 C.F.R. § 164.506(a) (2001). Also excepted are instances where care is received while an inmate. *Id.* at 506(a)(2)(ii).

53. Provider is defined quite broadly, incorporating definitions within 42 U.S.C. 1395x(u) and 42 U.S.C. 1395x(s) as well as "any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." 45 C.F.R. § 160.103 (2001) (defining health care provider).

disclosure for payment, treatment, or operations purposes.[54] The distinction between direct and indirect treatment relationships is that in the latter, care is provided as a result of another's orders, and the service, product, or treatment result typically passes to the initiating provider, who then supplies them directly to the individual.[55]

Under the initial final rule, a direct treatment relationship is likely to exist between the individual and the pharmacist. The Rule includes as health care providers anyone "who furnishes, bills, or is paid for health care in the normal course of business."[56] Since health care includes the "sale or dispensing of a drug . . . in accordance with a prescription,"[57] this naturally includes pharmacists. Although the pharmacist supplies medical care pursuant to a physician's orders, he or she typically passes the medication on to the consuming individual directly. Therefore, the pharmacist would have a direct treatment relationship with the individual and be bound by the same rules as the initiating physician who prescribed the medication.

The person who withdraws blood and subsequently performs tests would not have had a direct treatment relationship with the individual from whom the blood was withdrawn because both prongs of the "indirect treatment relationship" definition are satisfied. The venipuncture and testing are ordered by another provider, and the results typically are passed on to individuals through the treating physicians. Since these subsequent providers have only an indirect treatment relationship with the individual, the prior consent rule would not apply; providers with only an indirect treatment relationship could have used or disclosed health care information for treatment, payment, or operations purposes without the individual's consent.[58]

The lack of additional consent for disclosures made in connection with the treatment by and payment to the indirect provider may be acceptable because consent may have been presumed. Both resulted from the natural flow of events in connection with the patient's medical care. The patient was aware of the initial provider's determination that further testing was necessary for good patient care and voluntarily undertook that further care by another provider. The natural expectation would be that information would flow to the indirect provider specific to the patient's treatment and, moreover, that some

54. 45 C.F.R. § 164.506(a)(2) (2001). A discussion of governmental power to invade privacy and whether the correct balance has been drawn between governmental need for the information and individual privacy rights is beyond the scope of this Article.

55. 45 C.F.R. § 164.501 (2001) (defining "direct treatment relationship" and "indirect treatment relationship").

56. 45 C.F.R. § 160.103 (2001) (defining "health care provider").

57. *Id.* (defining "health care").

58. 45 C.F.R. § 164.506(a)(2)(i) (2001).

information would need to be exchanged in order that the indirect provider be paid by the patient's insurer.

The same logic may not apply with respect to information disseminated for the provider's health care operations. Unlike disseminations made in the context of treatment or payment, health care operations are primarily concerned with entity matters rather than with patient care.[59] Therefore, the nature of a consumer's consent to the spread of private information, the focus of which may not involve a benefit of services that was the *quid pro quo* of entry into the health care mini-society, differs. Here, the lay individual may be quite unaware of the extent of allowable purposes of information dissemination. Therefore, the individual would lack the ability to assess the trade-off between accepting care and entity-controlled information sharing.

One might suggest that the opportunity for reasoned choice was present, either because of a consent form signed at the time of enrolling in the health care package that would eventually reimburse the indirect provider for services, or because a savvy health care consumer would invoke his or her right to request a notice of disclosure practices directly from the indirect provider.[60] In the former situation, the separation in time from the original signing would likely inactivate a level of awareness sufficient to affirm informed consent as to the later transaction, especially since whatever was explained in the notice accompanying the consent form would have been of general application,[61] divorced from the current health concern or its potential stigma. At this later point in time, the patient might not even know what information has been made a part of his record and passed on.[62] As for the latter, even if the consumer requested and digested the indirect provider's notice, there would be no right to withhold consent because no consent was required.[63] The individual's choice would be limited to selecting another indirect provider to deliver the desired services. But, to the extent that individuals have a limited choice of caregivers or if available indirect providers employ the same practices, then where is the voluntary exchange of information for care in the context of health care operations?

---

59. *See* Gostin & Hodge, *supra* note 35, at 1477-78.

60. *See* 45 C.F.R. § 164.520(a) (2001).

61. *See Id.* Even authorizations may fail to provide adequate privacy protections since the forms provided for signature may be "blanket authorization[s]" allowing for unfettered access to the unsuspecting patient's records. Scott, *supra* note 22, at 490.

62. Gostin & Hodge, *supra* note 35, at 1467-68. Furthermore, since providers need not limit disclosure to the minimal necessary in the treatment context, 45 C.F.R. § 164.502(b)(2)(i), the indirect provider may be privy to far greater information than the individual would suspect.

63. 45 C.F.R. § 164.506(a)(2)(i) (2001).

In light of the above discussion, one must conclude that uses and disclosures connected with indirect caregivers are not negotiated. Instead they are permissive.[64] Permissive disclosure increases the risk of widespread sharing of the information because the information may be passed along without action or inaction on the part of the individual who is the subject of the information.[65] This practice, coupled with a potential lack of justification for the initial collection of information,[66] magnifies vulnerability to exposure. Thus, in the absence of individual control, privacy appears unprotected.

What about the larger context, where the initial final rules required consent in advance of uses or disclosures for treatment, payment, or health care operations?[67] At first glance, the consent requirement suggests that the exchange of consent for participation satisfies the elements of a voluntary negotiation between the parties.[68] However, the initial final rule permitted health care providers to condition treatment on consent, and health plans to condition enrollment on the provision of consent.[69] Consent, particularly in the context of enrollment, may not necessarily have been voluntary.[70]

Individuals often have little say in selecting a health plan; choice may be limited to pre-selected benefits offered as part of the individual's employment package.[71] Refusal for many may not be a viable option. To the extent that this is true, consent would not be voluntary despite the intentional execution of the consent form.[72] To explain: If a person is able to afford private health care without the benefit of insurance, then that person may experience the influence, but not coercive effect of the incentive to sign (in exchange for coverage).[73] The average person, however, is likely to suffer from inadequate care without coverage.[74] The latter would experience more than mere influence

64. *See* Fedder, *supra* note 15, at 570.
65. *See id.* at 571.
66. Gerald S. Schatz, *Health Records Privacy and Confidentiality: Pending Questions,* 18 J. CONTEMP. HEALTH L. & POL'Y 685, 689 (2002).
67. 45 C.F.R. § 164.506(a)(1) (2001).
68. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You,* 52 STAN. L. REV. 1049, 1111 (2000) (where contracts and statutory constraints against disclosures may provide adequate privacy protections).
69. 45 C.F.R. § 164.506(b)(1), (2) (2001).
70. *See* Fedder, *supra* note 15, at 570.
71. *See* GEORGE J. ANNAS, SOME CHOICE: LAW, MEDICINE AND THE MARKET 46 (1998); *see also* William M. Sage, *Regulating Through Information: Disclosure Laws and American Health Care,* 99 COLUM. L. REV. 1701, 1731 (1999) (stating 78% of employers offer only one plan).
72. *See* FADEN ET AL., *supra* note 38, at 256-60.
73. *See id.* at 258-59.
74. In addition to having to pay out-of-pocket each time, the uninsured's charges may also be significantly higher. For example, in a recent bill, the insurer, under a contract with the provider, was charged $13.33, which was the contractually es-

over a decision to execute the consent agreement; it would be tantamount to coercion because the subject who simply cannot afford needed care otherwise would be unable to resist the manipulation.[75] The coercive nature of the arrangement indicates that privacy is not adequately protected because the subject has insufficient control over the exchange.[76] If the consent is not effective in controlling disseminations, then the practical effect is nothing more than providing notice of data sharing practices.[77]

In response to criticisms,[78] the Final Rule was modified on August 14, 2002[79] to eliminate the consent requirement.[80] Instead, an individual has only a limited right to notice.[81] Therein, the individual is

---

tablished fee for the service. The insured was charged a mere additional $1.33. This total was substantially less than the amount that would be owed for the same service by an uninsured individual ($117.95). Moreover, the insurer ensured that extra charges that customarily get rolled into the service are eliminated from a bill. "Venipuncture" is a prime example. A representative bill charged $14.75 for the service of inserting a needle into the subject's skin for the purpose of inserting the medication that was listed as a separate charge. An uninsured individual, unlike an insured, would have to pay the additional charge. (Records on file with author).

75. *See* FADEN ET AL., *supra* note 38, at 258-59. Some have criticized the Rule directly, concluding that industry practices constituted "coerced consent." Scott, *supra* note 22, at 522.
76. *See* Gostin, et al., *supra* note 13, at 1132.
77. Gostin & Hodge, *supra* note 35, at 1468.
78. *See* INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY, *supra* note 26. In addition to the "forced consent" argument, segments of the health care industry have put intense pressure on HHS to eliminate the consent requirement, complaining of an inability to provide timely care and the burdensomeness of the paperwork. *Id.* Additional concerns included inefficiency through duplication of information provided by the Notice and in being unable to obtain advance diagnostic information. Jennifer Guthrie, *Time is Running Out - The Burdens and Challenges of HIPAA Compliance: A Look at Preemption Analysis, the "Minimum Necessary" Standard, and the Notice of Privacy Practices,* 12 ANNALS HEALTH L. 143, 169 (2003).
79. Standards for Privacy of Individually Identifiable Health Information, 67 F.R. 53182-01 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160 and 164). The effective date of the modified Final Rule was Oct. 15, 2002. *Id.*
80. *See* 45 C.F.R. § 164.506 (2002). The modification did *permit* entities to seek consent for use/disclosure for purposes of treatment, payment, or health care operations. 45 C.F.R. § 164.506(b) (2002). However, this may have been in response to confusion over meeting the demands of the Rule as well as physician confidentiality ethics. *See* Hippocratic Oath, MOSBY'S MEDICAL, NURSING, & ALLIED HEALTH DICTIONARY 817 (6th ed. 2002) (articulating a duty of confidentiality in the Oath as "[a]ll that may come to my knowledge in the exercise of my profession . . . which ought not to be spread abroad, I will keep secret . . . ."). The Health Privacy Project views the elimination of the consent requirement as undermining autonomous decisionmaking. BNA, *Business Groups Applaud Proposed Changes in Privacy Rule; Privacy Groups Disappointed,* 11 BNA's HEALTH LAW REPORTER 686 (May 9, 2002), *available at* http://ippubs.bna.com/ip/BNA/hlr.nsf/is/a0a5n1u4f2 (last visited July 9, 2002).
81. 45 C.F.R. § 164.520 (2002).

informed of entity use and disclosure practices and participant rights.[82] Is mere notice sufficient to protect privacy?

B. Notice as Privacy Protector

Ideally, privacy is best protected when the subjective values of individuals allow the exchange of information for health care benefits to be negotiated by the mechanism of informed consent.[83] Individualized control, however, presents serious consequences for discreet societies such as the organized health care system. If each participant were permitted to define his or her own parameters regarding the flow of information, the system itself could become inefficient[84] and undesirable.[85] Individualized disclosure practices could result in treatment inconsistencies or even harm. Vital communication between diagnosing and treating providers could be delayed or blocked. Fraudulent payments could not be prevented. In short, how could an organized system fulfill the defined objectives of efficient, non-fraudulent health care delivery[86] if the society lacked a degree of operational uniformity? How can one reconcile the uniformity needed for participation in a closed society such as an organized health care system with maintaining privacy?

If one considered only the subjective model of privacy, it would be difficult to see how the two could co-exist. To end the inquiry there would be unsatisfying. Perhaps a narrower question should be addressed that reflects the narrower context of the society defined as an organized health care system. Participation in it, unlike a broader form of society, requires something other than a series of non-related interactional opportunities where one may choose at each juncture whether to participate.[87] In the context of an organized health care system, such individual control over each transactional detail would defeat the existence of the defined society. To support the society itself, then, full individualized control must yield. But to what? If entities that control use and disclosure of health information were to determine all the terms of the agreement, then where is the *quid pro quo* gained by the collective individuals in exchange for the health information they provide the holders? Terms of participation must instead bear a resemblance to what privacy would be sacrificed in accord with the collective desire of individual participants.

---

82. *Id.* at 520(b).
83. *See* Fedder, *supra* note 15, at 570. *But see* Schwartz, *supra* note 10, at 4 (referring to Posner & Epstein's assertion that economic efficiency and social utility suggest full disclosure as preferred).
84. Fedder, *supra* note 15, at 571.
85. Gostin, *supra* note 9, at 17.
86. 42 U.S.C. § 1320-d n (1996).
87. *See* WESTIN, *supra* note 40, at 13, 21 (1967).

Measurement of the collective desire poses some problem. There is no absolute standard because choice varies with the individual. Some may be willing to give up more information than needed for entry into the defined society. Others would attempt to maximize beneficial interests of participation and minimize the sacrifice of control over personal information.[88]

Tort law resolves the issue by defining acceptable or unacceptable privacy loss in terms of reasonableness. Individual desire regarding invasion of privacy yields to the more objective measure of what would be highly offensive to a reasonable societal participant.[89] In more narrowly defined social contexts such as the workplace, where individuals have constructive (or actual[90]) notice that absolute privacy does not exist,[91] reasonableness is further limited by employer need. For example, suppose the employing entity wished to install surveillance cameras to prevent theft or to require drug testing to maintain a drug-free environment. If the expressed needs were legitimate, it would be unreasonable for persons to be highly offended by a loss of privacy in pursuit of those justifiable interests.[92] The acceptable loss to privacy, however, would extend only as far as that minimally required to meet the competing entity need.[93]

The organized health care system parallels the workplace context: A group of participants is brought together by a shared desire to obtain some benefit conferred by the involved entity and, in the exchange, will experience diminished privacy. As with workers, health care participants must receive some notice qualifying vulnerability. To bear a resemblance to the collective desire regarding reasonableness of the loss of privacy, the notice must reflect the opposing needs

88. This human propensity toward self-interest that results in gaining access to some good without a fair pro rata sacrifice presents a "free rider" issue. *See* Glyn S. Lunny, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millenium Copyright Act,* 87 VA. L. REV. 813, 859 (2001). Some individuals may also be more sensitive to revealing private information – a subjectively differing scheme that is at the heart of the issue regarding the exchange of privacy loss and entry into the system.

89. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977).

90. Employees are often provided actual notice that employers reserve the right to monitor e-mail correspondence. *See* Micalyn S. Harris, *Is EMail Privacy an Oxymoron? Meeting the Challenge of Formulating a Company EMail Policy,* 16 ST. JOHN'S J. LEGAL COMMENT. 553, 556-57 (2002). Employer needs to monitor include a variety of legitimate interests such as avoiding libel and maintaining worker productivity. *Id.* at 557.

91. *See, e.g.*, Sanders v. American Broad. Cos., Inc., 978 P.2d 67, 69 (Cal. 1999).

92. *See, e.g.*, Wilcher v. City of Wilmington, 60 F. Supp. 2d 298 (D. Del. 1999) (drug testing); Frye v. IBP, Inc., 15 F. Supp. 2d 1032 (D. Kan. 1998) (drug testing); Acuff v. IBP, Inc., 77 F. Supp. 2d 914 (C.D. Ill. 1999) (theft surveillance).

93. *E.g., Acuff*, 77 F. Supp. 2d at 914 (including jury question as to excessiveness of surveillance by use of wide-angle lens).

that warrant the incursions, and the incursions should not extend beyond the minimum needed.[94]

The Privacy Rule, which articulates the contents of the notice[95] and permissible incursions,[96] should thereby reflect a reasonable balance.[97] In turn, this permits diminished privacy to comport with the collective desire and signify that privacy has adequately been protected. Thus, the underlying construct in analyzing whether the Rule adequately protects the privacy of individual participants will be premised on a necessity for the invasion of privacy and some notice regarding the invasion. Since individuals within an organized health care system have a reasonable expectation that entities will keep information confidential,[98] notices provide a means whereby individuals may judge whether to participate in the mini-society using, as criterion, the usage/disclosure *quid pro quo*. Notice thereby guards privacy to the extent that individuals may meaningfully decide whether to participate, understand the exchange, and to the extent that the exchange reflects the proper balance.

C. Notice Under the Rule

The importance of this section is that it requires covered entities to explain to individuals what is offered as the *quid pro quo* for participation in the mini-society. Notice is important to encourage participation in the system, particularly since the technological age allows for intrusive gathering and sharing of information at massive rates. Without notice of data practices, the crucial public trust is unlikely to exist. For purposes of evaluating the privacy issue, the practices evidenced in the notice must reflect the appropriate *quid pro quo*.

It is essential to keep in mind that the main purpose of the HIPAA authorized regulations is not to ensure the privacy or confidentiality of medical records, but to reduce the administrative costs of federally run health care programs.[99] Specifically, the Rule is meant "to im-

94. Gostin and Hodge frame the balance in terms of individual privacy versus the "common good." Gostin & Hodge, *supra* note 35, at 1439.

95. *See* 45 C.F.R. § 164.520 (2001).

96. *See generally* 45 C.F.R. § 164.502 (2001).

97. *See* Ian Goldberg, et al., *Trust, Ethics, and Privacy,* 81 B.U. L. REV. 407, 418-19 (2001). The authors focus on "fair information practices" to determine whether disclosure practices are ethical. Notice, minimization, limited use, and provision of choice to withhold consent form the main components of what the authors consider fair information practices. *Id.* Those components are also primary balancing factors.

98. Gostin, et al., *supra* note 13. *The Nationalization of Health Information Privacy Protections,* 37 TORT & INS. L.J. 1113, 1118 (2002).

99. Final Privacy Rule Preamble – Background and Purpose, 65 Fed. Reg. 82,461 – 82,510 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160 – 164), *available at* http://www.aspe.hhs.gov/admnsimp/final/PvcPre)!.htm. (last visited June 1, 2001) (referring to the enabling provisions within § 261 and § 1172(b) of § 262 of

prove the Medicare program . . ., the Medicaid program. . ., and the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[100] This, then, articulates entity need. The Privacy Rule was mandated because the success of the program hinged on its inclusion.[101]

Formerly, when records were maintained in hard copy files, there was both a perception of confidentiality and, in reality, a low risk of breaches of confidentiality due, at least in part, to the expense barrier of accessing and using those records.[102] As technological advances allow for cheap and easy access to records, both perception of vulnerability and real exposure to privacy violations increase.[103] Statistics revealed a high degree of public fear about the transmission and storage of private health information.[104] This signaled concern that participants might not provide accurate health information or submit to treatment that would expose their private health information unless they were assured that their private health information would be kept

---

the enabling statute HIPAA § 262. The Congressional "recommendations" regarding health information privacy appear in the same subtitle as the objective of cost efficiency. HIPAA, § 264, (Subtitle F – Administrative Simplification). This supports the view that such protections are necessary to promote the overall efficiency objectives.

100. HIPAA, § 261; *see also* Final Privacy Rule Preamble – Background and Purpose, 65 Fed. Reg. 82,461 – 82,510 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160 – 164), *available at* http://www.aspe.hhs.gov/admnsimp/final/PvcPre)!.htm. (last visited June 1, 2001) (promoting electronic commerce). Many countries, especially in Asia, have developed or are currently developing laws in an effort to promote electronic commerce. These countries recognize consumers are uneasy with their personal information being sent worldwide. Privacy laws are being introduced as part of a package of laws intended to facilitate electronic commerce by setting up uniform rules.

101. Final Privacy Rule Preamble – Background and Purpose, 65 Fed. Reg. 82,461 – 82,510 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160 – 164), *available at* http://www.aspe.hhs.gov/admnsimp/final/PvcPre)!.htm. (last visited June 1, 2001).

102. *Id.*

103. *See* A. Michael Froomkin, *The Death of Privacy?* 52 STAN. L. REV. 1461 (2000) (contending new technologies devastate privacy).

104. For example, polls show that Americans fear loss of control over private medical information. Final Privacy Rule Preamble – Background and Purpose, 65 Fed. Reg. 82,461 – 82,510 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160 – 164), *available at* http://www.aspe.hhs.gov/admnsimp/final/PvcPre)!.htm (last visited June 1, 2001); *see also* Princeton Survey Research Associates, *Confidentiality of Medical Records: National Survey (Summary and Overview)* (1999), *available at* http://www.chcf.org/documents/ihealth/survey.pdf (last visited April 2, 2002). Fifty-four percent of United States adults believed that the "most serious threat to medical privacy" stems from the computerization of medical records. *Id.* Computer hackers posed a major fear. *Id.*

confidential.[105] The Congressional purpose of efficient health delivery would be impossible without the cooperation of the participants. Thus, the development of public trust through assurances that privacy would be maintained was vital to the success of the program. Without it, individuals would be unwilling to share the very information that is required.[106] Need, therefore, must be defined in terms of what privacy must be lost in order to make the system work effectively.

In both the initial final rule and the modified final rule, section 164.520, the Notice provision, obligates covered entities to inform individuals how information about them may be used and disclosed if they are to participate in the organized health care management mini-society.[107] Individuals are told, in writing, how the individually identifiable health information that they understand to be "protected health information" may be used and disclosed.[108] Notices must describe, in plain language, potential uses and disclosures, with one use or disclosure example to accompany descriptions in each of three categories: treatment, payment, and operations.[109] Information regarding the individual's rights and the covered entity's duties, as well as instructions on how to contact the person providing the notice, must be listed.[110] In addition, the notice must inform individual participants that revocable authorizations will be required prior to most other uses or disclosures.[111]

---

105. *See, e.g.*, Phillip C. Buttell, *The Privacy and Security of Health Information in the Electronic Environment Created by HIPAA*, 10 KAN. J.L. & PUB. POL'Y 399, 406 (2001).

106. Final Privacy Rule Preamble – Background and Purpose, 65 Fed. Reg. 82,461 – 82,510 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160 – 164), *available at* http://www.aspe.hhs.gov/admnsimp/final/PvcPre)l.htm (last visited June 1, 2001); *see also* Janlori Goldman & Zoe Hudson, *Virtually Exposed: Privacy and E-Health*, *available at* http://www.chcf.org/topics/view.cfm?itemID=12562. Trust is uneven among entities. Americans have been far more likely to trust health care providers such as physicians and hospitals with their personal information (60%) than they do government health insurers (35%). Princeton Survey Research Associates, *supra* note 104.

107. 45 C.F.R. § 164.520(a) (2001); 45 C.F.R. § 164.520(a) (2002).

108. 45 C.F.R. § 164.520(b) (2001); 45 C.F.R. § 164.520(b) (2002).

109. 45 C.F.R. § 164.520(b)(1)(ii)(A)&(B) (2001); 45 C.F.R. § 164.520(b)(1)(ii)(A)&(B) (2002).

110. 45 C.F.R. § 164.520(b)(1) (2001); 45 C.F.R. § 164.520(b)(1) (2002).

111. 164.520(b)(1)(ii)(B)&(E) (2002). Prior to the August, 2002 modification, the notice would have contained an additional description of each purpose for which no prior consent or authorization was needed. 45 C.F.R. § 164.520(b)(1)(ii)(B) (2001). The elimination of the consent provision reflects the removal of any consent requirement in the modified version. *Cf.* § 164.512 (2001), *with* § 164.512 (2002). The 2002 version merely permits consent 45 C.F.R. § 164.506(b), presumably to assure doctors that compliance with the regulations is compatible with physician ethics. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14776, 14779 (March 27, 2002) (describing modifications of pro-

Some weaknesses are evident despite the comprehensive notice requirements. For example, in contrast to consent requirements, notice provisions provide no functional opportunity for informed discussion of relevant issues.[112] This may be exacerbated by the lack of an obligation to provide notice of uses and disclosures specific to the particular entity, either in the description or in the example. Instead, covered entities need only provide "sufficiently detailed" descriptions[113] of uses and disclosures that are permissible under the Rule. Entities may thereby be encouraged to develop boilerplate laundry lists and utilize innocuous examples that may mask more controversial uses and disclosures.[114] As a result, the listings may not be particularly helpful to individual consumers. The document may be too overbroad to be of much value, or too lengthy for consumers to attempt to read and understand. Absent awareness, privacy is inadequately safeguarded.[115]

The timing of the notice may create a gap between an individual's understanding of potential uses and disclosures at the time of receipt and the time when information is gathered, re-configured, and disclosed subsequently. This may be exacerbated by the intermittency of the notice. Notice is only provided at specified intervals such as at the time of enrollment,[116] or upon a first visit,[117] for example. When individuals receive subsequent treatment, especially some time after the original notice, they may not have in mind the specifics that apply to the current procedure. Given the laundry listing that would be appropriate upon initial notice, the individual may lack awareness of the intensity of the dissemination at the time when a certain level of privacy may be presumed by the individual but not in reality realized.[118]

In essence, the regulatory notice requirements reveal that the covered entities have extensive control over information dissemination,

---

posed Rule codified at 45 C.F.R. pts. 160, 164), *available at* http://www.hhs.gov/ocr/hipaa/propmods.txt (last visited April 2, 2002).

112. Guthrie, *supra* note 78, at 172. Even the mechanism ascertaining receipt of notice is lax. *Id.* at 172-73.

113. 45 C.F.R. § 164.520(b)(1)(ii)(D) (2002).

114. *See* discussion of marketing strategies *infra*. Inconsistency between practice and policy is hardly new. Scott, *supra* note 22, at 485-86. The generalities permitted under the Rule appear to allow for a variation on the theme.

115. *See* Schwartz, *supra* note 10, at 5.

116. 45 C.F.R. § 164.520(c)(1)(B) (2002) (for health plans). Health plans must also provide notice no later than by compliance date for current enrollees and after material revision. 45 C.F.R. § 164.520(c)(1) (2002). All entities must provide notice to any person who requests the information. 45 C.F.R. § 164.520(c) (2002).

117. 45 C.F.R. § 164.520(c)(2) (2002) (for health care providers offering direct treatment). Proof of receipt of the notice provision from providers lies in the written acknowledgement or the provider's documentation of good faith efforts and explanation of why the acknowledgement was not received. *Id.* at 520(c)(2)(ii).

118. *See* Schwartz, *supra* note 10, at 48-49 (describing the consumer belief that health information enjoys a high level of protection is misplaced and exploited).

subject only to the limits of the regulation. These are explained in greater detail elsewhere in the Rule. To the extent that actual uses and disclosures of a particular entity do not closely correspond with the "sufficiently detailed" descriptions and examples, the notice lacks information relevant to individuals to make subjective-based decisions trading privacy for benefit. On the other hand, if the descriptions of permissible disclosures comprise a *quid pro quo* representing the trade apropos the collective desire, then it matters not the specific uses and disclosures made by any particular entity. All that would matter for privacy to be respected would be that the descriptions reflected collective desire. The notice thus performs the dual function of developing trust through information and inculcating an attitude of reasonableness. Uses and disclosures made in conformity with the Rule thereby grant entities immunity from liability because the specific provisions describe the manner in which privacy may legally be invaded by the covered entity. The Rule should thereby provide the objective measure of what would be highly offensive to a reasonable societal participant.

The analogy works provided that the Rule mirrors the appropriate *quid pro quo* of lost privacy for efficient management of the organized health care system mini-society. This occurs when the incursion on individual privacy is no greater than necessary to attain the primary interests of the system. In this case, Congress has defined those interests as programmatic efficiency and effectiveness in maintaining public health.[119]

D. Overview of Privacy Incursions

Section 164.502 of the modified Final Rule sets out the basic rule regarding uses and disclosures of protected health information.[120] The essential message appears to convey a warning to covered entities to be on guard since use and disclosure is permissible only as described.[121] As details unfold, one has the impression that the primary function of the regulations focuses not on maintaining individual privacy, but on offering red light/green light guidance to covered entities. That is, to specify how to proceed without liability. This impression is affirmed by the inability of the individual to learn how or to whom

119. *See* HIPAA, § 261 note; *see also* Final Privacy Rule Preamble – Background and Purpose, 65 Fed. Reg. 82,461 – 82,510 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160 – 164), *available at* http://www.aspe.hhs.gov/admnsimp/final/PvcPre01.htm (Privacy laws enhance electronic commerce in the United States and abroad by removing consumer uneasiness); *see also* David Banisar, *Privacy and Human Rights 2000*, *at* http://www.privacyinternational.org/survey/phr2000. Trust is fostered by protecting privacy interests.

120. 45 C.F.R. § 164.502 (2002).

121. 45 C.F.R. § 164.502(a) (2002).

certain of his or her private information has been disseminated[122] and by the absence of a private right of action against any wrongdoing entity.[123]

Section 164.502 organizes the regulatory scheme into ten use and disclosure categories, the first of which describes the general framework.[124] Each is discussed in greater detail in subsequent provisions, as is the scope of disclosure.[125] Additional provisions govern how disclosures may be made without fear of entity liability when recipients

122. *See* 45 C.F.R. § 164.528(a) (2002). Three problematic uses or disclosures that are permitted by section 164.502(a) and to which an individual is not entitled to an accounting include those made for health care operations, 45 C.F.R. § 164.528(a)(1)(i) (2002), those made pursuant to authorization, 45 C.F.R. § 164.528(a)(1)(iv) (2002), and when information has been transmitted without certain personal identifiers, 45 C.F.R. § 164.528(a)(1)(viii) (2002) (referring to the limited data set of § 164.514(e)).

Covered entities may use PHI to create (or to have business associates create) limited data sets. 45 C.F.R. § 164.514(e)(3)(ii) (2002). The data sets compile targeted PHI information absent regulation-specified identifiers including names, street address, phone, fax, and social security numbers, and some other common identifiers such as those attached to vehicles, photographs, or biometric identifiers. 45 C.F.R. § 164.514(e)(2) (2002). Once the information is organized into data sets, the entity may use or disclose the sets for health care operations. 45 C.F.R. § 164.514(e)(3)(i) (2002).

Although it would appear to be protective of the sensitive information, there is a back door that enables re-identification. 45 C.F.R. § 164.514(c) (2002) (codes may be used to allow for re-identification). Although the drafters acknowledge transmission and re-identification, the individual is unlikely to become aware of the dissemination because the regulations also prohibit those who do so to make contact with the individual. 45 C.F.R. § 164.514(e)(5) (2002). Interestingly, the same passage that prohibits contacting also prohibits the activity that would be the necessary precursor to the contact. *Id.*

123. *See* HIPAA, § 262.

124. 45 C.F.R. § 164.502(a) (2002). Use and disclosure by a covered entity is permitted in conjunction with the following stipulations: made to the individual; for treatment, payment, or health care operations; with proper authorization or agreement; when permitted or required by law; for fundraising and underwriting purposes; when the information is transmitted as a limited data set with certain direct identifiers removed; and when regulatory-specified safeguards are established, including the transmission of only the minimum necessary information in most instances. *Id.*

125. 45 C.F.R. § 164.502 (2002). Unless excepted, disclosing entities must make "reasonable efforts to limit protected health information to the minimum necessary to accomplish the purpose" and must comply with notice provisions, if any are required. 45 C.F.R. § 164.502(i) (2002). Other provisions of section 164.502 require entities to uphold heightened privacy agreements voluntarily undertaken (c); permit the creation of de-identified information (d); provide rules regarding those deceased (f), legally represented by another (g), requesting special means of communication (h), or disclosing as whistleblowers (j). Exceptions are for treatment, to the individual, in conjunction with most authorizations; to report possible entity wrongdoing, and when the information is required by law for judicial or administrative proceedings, domestic violence, or law enforcement purposes. *Id.* at 502(b).

are business associates not covered under the regulations.[126] Subsequent provisions in sections 164.504 through 164.528 primarily expand on the initial themes and further explain the many exceptions and exclusions.

1. *Disclosures for Treatment, Payment, and Health Care Operations*

Disclosures for treatment, payment, and health care operations are permissive under the Rule. Therefore, they warrant special attention in determining whether privacy is adequately safeguarded. The notice must inform individuals that entities have a permissive right to use and disclose the individual's protected health information for purposes of treatment, payment, and health care operations. To assist with understanding, the labels must be accompanied by a description that includes at least one example for each category.[127]

a. Payment

It is fairly obvious that the obligor must provide payment in reference to the provided care in order to ensure the continued financial stability of the system and its members. The exchange of information in support of payment is inevitable to avoid fraud – a primary Congressional interest in imposing the regulatory scheme. Analogous to the circumstance in the initial final rule where no consent was required before disclosures connected with payment to indirect providers, a use or disclosure in pursuit of this interest satisfies the *quid pro quo* that would be reasonable as long as the information that were used or disclosed for payment purposes minimized the exposure of the participant's private information.

The Rule suggests minimizing individual exposure since its standard requires that information may be disclosed for purposes of payment only to the extent that is the minimum necessary.[128] Although strict liability would protect individual privacy to its fullest, as in other privacy claims, such heightened protection does not exist. Covered entities are charged with exercising "reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request [for information]."[129] "Reasonable effort" will be defined in court. Until it is known how liberal entity disclosure practices will pass muster under

126. *Id.* at 502(e). Disclosures to business associates under an entity-associate contract are considered to be "regulatory gaps" because the HHS has no authority to regulate the associates. However, the gap is addressed by requiring entity contracts to maintain confidentiality provisions. Scott, *supra* note 22, at 524-26.

127. 45 C.F.R. § 164.520(b)(1)(ii)(A) (2002).

128. 45 C.F.R. § 164.502(b) (2001); 45 C.F.R. § 164.502(b) (2002).

129. 45 C.F.R. § 164.502(b)(1) (2002).

the court rulings, the extent to which individual privacy rights will be protected cannot be assessed.[130]

b. Treatment

As with payment purposes, adequate treatment can occur only with proper disclosure of private health information.[131] Unlike for payment purposes, reasonable individuals are likely to prefer trusted health care providers, who already have a duty to maintain patient confidentiality,[132] to have access to more rather than less information in order that accurate diagnoses and treatments can be administered. Presumably, an individual would agree to far greater exposure of health information in order to derive the maximum benefit of participation. Therefore, the collective desire of individual participants would likely not restrict private health information to the minimum.[133] This accords with the Rule standards that except health care providers from the "minimum necessary standard" when information is used or disclosed for treatment purposes.[134] Because the Rule appears to comport with collective desire, privacy is safeguarded in the treatment context.[135]

c. Health Care Operations

Health care operations includes a host of activities including quality assessment; reduction of costs; contacting patients about treatment alternatives; evaluating provider and health plan performance; training non-health care professionals; health insurance contract concerns; and business and administrative activities.[136] Special atten-

130. Even commentators whose perspective is oriented toward burdensomeness to industry find the "reasonableness" provision confusing. *See, e.g.*, Guthrie, *supra* note 78, at 166. Clearly, the standard will vary from entity to entity. Kevin B. Davis, *Privacy Rights in Personal Information: HIPAA and the Privacy Between Fundamental Privacy Rights and Medical Information,* 19 J. MARSHALL J. COMPUTER & INFO. L. 535, 551 (2001).

131. *See* Sage, *supra* note 71, at 1785.

132. *See* Guthrie, *supra* note 78, at 158-59.

133. *See* Gostin, *supra* note 9, at 28. The trade-off, diminishing autonomous choice, is desirable when it relates to improving overall health. *Id.* Therefore, collective desire may be implied.

134. 45 C.F.R. § 164.502(b)(2)(i) (2001); 45 C.F.R. § 164.502(b)(2)(i) (2002). Other circumstances in which the minimum necessary standard does not apply include the following: disclosure to the individual, pursuant to a valid authorization under limited circumstances; to the HHS Secretary for compliance and complaint investigations; and for those required by law. *Id.* A discussion regarding the disclosures required by law could alone be the subject of a paper and is beyond the scope of this paper.

135. *But see* Schwartz, *supra* note 10, at 69-70 (stating treatment provides a unique opportunity for abusive disclosures).

136. 45 C.F.R. § 164.501 (2002) (defining "health care operations").

tion should be directed toward health care operations as distinct from marketing activities to determine whether they represent an appropriate *quid pro quo* of entity control over private information in exchange for benefits that individuals receive by participating in the health care mini-society.

Significantly, marketing generally requires authorization prior to use or disclosure of private health information[137] while operations activities do not.[138] Requiring authorization tacitly acknowledges that, in the marketing context, entity benefit is the primary focus. Safeguarding privacy appears to warrant some individualized control over information dissemination to overcome the moral hazards created by industry's conflict-of-interest in making disclosure decisions.[139] To the extent that the Rule mandates individualized control in the context that consumers would collectively consider "marketing," privacy is protected. As will become apparent, these two activities (marketing and health care operations) seem to converge. As a consequence, the individual may very well be confused about the category in which a particular activity may be included and be unable to take action to avoid unwanted exposure.

(i). Modified Rule

The modified Rule begins with the standard that covered entities that wish to use or disclose protected health information for marketing purposes must obtain the individual's prior authorization.[140] If the marketing is sponsored by another entity through direct or indirect remuneration to the covered entity, the individual must be forewarned by a statement within the authorization document.[141] This standard of permitting the individual to exercise control through information and choice is consistent with a key privacy protection ingredient. Therefore, on the surface, the Rule appears to adequately safeguard privacy. Whether the appearance is manifest reality depends upon what is or is not included within the Rule's definition of "marketing" for which authorization is required and the extent to which an authorization document must be issued.

The Rule recognizes that communications made for the purpose of encouraging the individual to purchase or use advertised products or services are essentially marketing practices.[142] As indicated above,

137. 45 C.F.R. § 164.508(a)(3) (2002).
138. 45 C.F.R. § 164.502(a)(1)(ii) (2002).
139. *See* Goldberg, et al., *supra* note 97 at 416.
140. 45 C.F.R. § 164.508(a)(3)(i) (2002). Exceptions to the need for prior authorization are when the covered entity makes a face-to-face communication or provides a promotional gift of nominal value. *Id.*
141. *Id.* at (ii).
142. 45 C.F.R. § 164.501 (2002) (defining marketing).

use or disclosure of private information to assist in such practice generally requires the individual's prior agreement.[143] When the covered entity plans to sell the individual's private information to another entity that makes the marketing communication on its own behalf,[144] the authorization document must inform the individual that disclosures will be made in exchange for some sort of remuneration to the covered entity who holds the private health information.[145] The dual safeguards of knowledge and choice suggest adequate privacy protection. But does the scope of protection encompass all practices that lay individuals would consider marketing? What sorts of communications made for the purpose of encouraging the individual to purchase or use advertised products or services are excluded from the definition? Are there circumstances in which disclosures for what lay persons would consider marketing are permissible under the Rule absent agreement? Do remunerated disclosures always require the individual's knowledge or prior agreement? To the extent that the answers to the questions outline exceptions to the standard of no disclosures for marketing purposes without prior authorization, individual privacy is undermined.

(ii). Initial Final Rule

It may be helpful to compare the modified rule with its precursor to determine weaknesses within the Rule and ascertain cures. As in the modified rule, the marketing definition began with the general proposition that marketing communications were those that encouraged individuals to purchase or use products or services.[146] However, many communications made by a covered entity to encourage consumer use would not have been considered marketing.[147] In addition, there were some activities considered mere health care operations that the rule candidly stated were really marketing strategies. As such, they would not have required the individual's authorization prior to uses and disclosures made in conjunction with the defined conduct.[148] Communications excluded from the definition of marketing and marketing that fell within the rubric of health care operations will be discussed in turn.

143. 45 C.F.R. § 164.508(a)(3) (2002).

144. 45 C.F.R. § 164.501 (2002).

145. 45 C.F.R. § 164.508 (a)(3)(ii) (2002).

146. 45 C.F.R. § 164.501 (2001) (defining marketing).

147. *Id.*

148. *Id.* (defining "health care operations"). Section 164.514(e) describes what conduct needs no prior authorization.

d. Communications Not Considered Marketing

Several types of communication would not have been considered marketing under the Rule. Purely descriptive information that helped clarify for the individual what providers were included as part of the heath plan network would not have been considered marketing. Nor would descriptive information that informed the individual whether certain products or services were included within the plan's coverage.[149] These were retained in the modified version.[150]

Such communications have little impact on privacy concerns. The communication may be general and require no private information from the individual, or may be a foreseeable response to an individual regarding specific benefits of participation. The communication alone impacts no disclosure except when the individual volunteers it. The communication may impact privacy only in the intrusion sense – that is, that a person would consider the communication an undesirable intrusion into his sphere because he does not wish to be approached on the subject.

Another type of exclusion would have permitted communications tailored to the individual's circumstances. These could have been made without authorization or consent under two circumstances: if made orally or, if written, were not a result of remuneration from a third party.[151] A physician could freely discuss treatment alternatives and provide brochures supplied by companies whose products were featured therein as long as the outsiders gave no direct or indirect remuneration to the physician for making the communication.[152]

It would not be considered marketing for a physician to discuss alternative treatments with a patient or to offer the patient brochures or even samples. The brochures themselves could be designed to induce selection of their products over others, perhaps because of bulk-buying benefits, and yet not be considered marketing provided that the mid-

149. *See* 45 C.F.R. § 164.501(6)(v) (2001) (part (6)(v) of the definition of "health care operations").

150. *See* 45 C.F.R. § 164.501(1)(i) (2002) (part (1)(ii) of the definition of marketing).

151. 45 C.F.R. § 164.501 (2001) (defining marketing). This condition attaches to the descriptive function, but does not impact privacy in the disclosure sense. Instead, it may eliminate the incentive to direct the individual a product or service that benefits the entity rather than the individual.

152. *Id.* It is unclear exactly which covered entity is prohibited from receiving remuneration. If a physician is the communicator, is he or she the only covered entity that may not receive remuneration? Suppose the physician, who is a covered entity on his own, offers services under a health plan. Is the larger health plan entity also prohibited from receiving remuneration? Of course, the company could supply samples that might induce the physician to prescribe that particular brand because of the benefit that passes through the physician directly to the consumer by way of the free samples.

dleman physician has received no remuneration.[153] This appears to be unchanged in the modified version.[154] So far, no disclosure privacy issue is at stake because no protected health information is disseminated to a third party.[155] It is only a physician who makes use of information necessarily in his or her domain to assist the individual in selecting a course of treatment.

e. Disguised Marketing

Likewise, in the initial and modified versions, a health plan entity could write to the individual directly and enclose brochures provided by third parties who supply the advertised goods and services. This would not be considered marketing even though offered to induce the individual to change physicians, treatment center, or treatment, as long as the health plan receives no direct or indirect remuneration. Instead, it is likely to be considered within the scope of health care operations where entities are free to contact individuals about treatment alternatives.[156]

If the communicating entity does receive remuneration, even indirectly, then the communication is generally considered marketing.[157] Under the initial rule, remunerated marketing could still fall within the definition of health care operations if the entity "prominently" stated that it had or would receive remuneration, identified itself as the source of the communication, and supplied applicable opt-out information.[158] It could even target the individual.[159]

Remunerated marketing considered part of health care operations fell roughly within three categories: face-to-face communications, communications concerning products and services of "nominal value," and

153. *Id.* Providing alternative suggestions for cheaper remedies has been controvercial in the past. Scott, *supra* note 22, at 502.

154. *See* 45 C.F.R. § 164.501 (2002) (defining marketing at (1)(ii), (iii)). *But see infra* regarding changes.

155. Although disclosure privacy may be intact under these circumstances, the unfettered provision of information risks manipulating the consumer, in part because they may choose to provide only entity-oriented reduced cost alternatives or create demand for particular products or services. Sage, *supra* note 71, at 1788-89. Such communications, excluded from authorization requirements, are really a type of marketing, especially if entities gain the benefits of promoting less expensive items because of favorable contractors. There is a "fine line between information and propaganda." *Id.* at 1789.

156. 45 C.F.R. § 164.501 (2001) (part (1) of the definition of "health care operations"; part (2)(ii) of the definition of "marketing"); 45 C.F.R. § 164.501 (2002).

157. *See* 45 C.F.R. § 164.514(e)(3)(i)(B) (2001); 164.501(1)(i) (2002) (part (2) of the definition of "marketing"). However, if remunerated disclosures result in value-added benefits, they could be excluded from the definition of marketing. 45 C.F.R. § 164.501(1)(i) (2002) (part (1)(i) of the definition of "marketing").

158. 45 C.F.R. § 164.514(e)(3) (2001). There is no need for inclusion of an opt-out provision if the communication is a broad-based mail-out. *Id.* at 514(e)(3)(i)(C).

159. *Id.* at 514(e)(3)(ii).

communications concerning "health-related products and services."[160] The first circumstance, similar to a non-marketing communication, suggests that the encounter need not have been limited to oral communication. The last appears far broader in that it suggests that covered entities could mail, e-mail, fax, or phone the individual about a variety of products and services based on the individual's specific condition. Mail-outs or encounters could have included an extensive display of product information such as catalogues, fliers, and brochures, any of which may have been compiled based on remuneration from advertisers. How is the individual's privacy protected given the permissive regulatory provision regarding operational activities?

Let's say that an individual, John Doe, has just visited his physician for a condition that turns out to be diabetes. Let's imagine further that the physician has prescribed a specialized treatment different than the norm because of another of John's conditions - say quadriplegia,[161] for example - which makes the standard treatment inappropriate. The unrelated condition would have to be disclosed to the health plan entity under the "minimal necessary" rule along with diabetes. Otherwise, the plan would not authorize payment of the more expensive diabetic treatment. The health plan would now have protected information related not only to the immediate condition that needed attention, diabetes, but also to the unrelated condition that gave rise to the non-standard treatment plan.

Once the larger entity held the information, it could use or disclose it for health care operations, including marketing as described above. In preparing its marketing strategy for a mail-out or face-to-face encounter, the entity could share protected health information with a business associate who assisted in some way with the communication.[162] The business associate could be another covered entity such as a clearinghouse that compiled and organized the information, or it could be some non-covered entity that assisted in some undisclosed fashion. John and others could have been organized by type or class and targeted for mail-outs, e-mails, faxes, or conceivably door-to-door visits.[163] The agent could have been provided a list of names and addresses and told to discuss specific items tailored to the individual's needs.

Although sharing information intra-entity or with a business associate is held to a "minimum necessary" standard, must it be limited to

160. *Id.* at 514(e)(2).

161. Quadriplegia should fall within the definition of protected health information because it is information received by a provider or plan that either relates to one's physical condition, or for which one received some health care. 45 C.F.R. § 160.103 (2001) (defining "health information").

162. 45 C.F.R. § 164.514(e)(2)(ii) (2001).

163. *See* Gostin, *supra* note 9, at 27-28. Such provisions diminish privacy practices. *Id.*

John's diabetic condition? Use or disclosure should be limited to the "minimum necessary to accomplish the intended purpose."[164] If the intended purpose is to make efficient marketing communications subsumed under health care operations, would it not be necessary to and disclose all of John's conditions absent irrelevant details? The initial final rule merely required that marketing operations communications be of nominal value or concern "health-related products and services"[165] and, if the individual were targeted, that advertised goods or services "*may* be beneficial to the health of the type or class of [the] individual."[166] There was no proscription or requirement of an individualized approach; no standard defining how groups could be formed or classified; and no minimum qualification or quantification of benefit that might limit disclosures to business associates. Essentially, industry was left to define its own parameters.[167] Individuals could be lumped into a group in accord with some entity or business associate-defined classification. John could be placed in a category inclusive of diabetics, quadriplegics, quadriplegics with diabetes, or perhaps some other classification that might include other of his health conditions. The classification then dictated the communications John could receive under the rubric of heath care operations.

What type of communications could John have received? One could easily envision an entity sending a flier displaying a variety of wheelchair models by different companies who paid a fee to be included.[168] Could the definition of "health-related product" or "health-related service" also have extended to advertising of specially made vehicles that were wheelchair friendly, or to home constructors who specialized in outfitting homes with ramps and other modifications with the quadriplegic in mind? How far could the standard stretch before a product or service would be of no health benefit to the type or class of individuals targeted? Must "health" have included only physical health? If mental health forms a part of the picture, then, arguably, compiling and sending out information that eased the everyday difficulties brought about by the physical condition improved overall

164. 45 C.F.R. § 164.502(b)(1) (2001).

165. 45 C.F.R. § 164.514(e)(2)(i)(C) (2001).

166. 45 C.F.R. § 164.514(e)(3)(ii)(A) (2001) (emphasis added).

167. Such self-regulation does not adequately safeguard privacy. *See* Goldberg, et al., *supra* note 97, at 416 (discussing the conflict of interest between a data collector who wants the information for a particular use and a subject whom the data collector fears will not consent); *see also* Jessica Litman, *Information Privacy/Information Property,* 52 STAN. L. REV. 1283, 1283 (2000) (advocating for personal ownership of information and noting that industry regulation's protection of privacy was an "abject failure").

168. The entity name might even be viewed as an endorsement of the listed products and the remuneration notice could be as innocuous as: "We got a great deal on these products and are passing the savings on to you."

mental health.[169] If one accepted such a broad interpretation, then the illustrations above would have been permitted under the Rule's health care operations provisions. Disclosures related to commercial marketing thereby offers little privacy protection.[170]

(i). Modified Rule

Have the potential problems been fixed by the modified Rule? Do the modifications extend or further retract protections? A seemingly major change in the regulations was the omission (from the definition of "health care operations") of activities relating to business management and general administrative activities: "marketing for which an individual authorization is not required as described in § 164.514(e)(2)."[171] Section (e)(2) provided that no authorization was needed for uses or disclosures for marketing communications to the individual if they were made face-to-face, if it concerned products or services of nominal value, or if the communication about health-related products or services adhered to a specified standard.[172] The standard included entity self-identification, indication of any remuneration for the marketing communication, an explanation of how the product or service related to the individual's health if the individual was specifically targeted,[173] and instructions on how to opt out of receiving future communications.[174]

A careful examination of the apparent omission reveals that a substantial portion has merely been relocated to the revised Section 164.508, which directly deals with authorizations. Therein, face-to-face communications by a covered entity are excepted from the authorization requirement, as are nominal valued promotional gifts.[175]

Both the former and revised regulations use "nominal value" as a standard negating the requirement that use or disclosure occur sub-

169. The Rule carries no definition of health. "Health information" relates to "physical or mental health or condition." 45 C.F.R. § 160.103 (2001) & (2002) (defining "health information"). Therefore, the Rule may arguably permit the illustrated marketing within health care operations.

170. *See* Gostin, et al., *supra* note 13, at 1137.

171. 45 C.F.R. § 164.501(6)(v) (2001) (part (6)(v) of the definition of "health care operations"). Compare the modified version of the definition. 45 C.F.R. § 164.501 (2002).

172. 45 C.F.R. § 164.514(e)(2)(i) (2001). Disclosures could also be made to assist business associates. *Id.* at 514(e)(2)(ii).

173. 45 C.F.R. § 164.514(e)(3) (2001). If targeted, the communication must also explain why the individual was targeted. *Id.* at (e)(3)(ii)(B). It is not difficult to imagine an attractive phrase.

174. 45 C.F.R. § 164.514(e)(3)(i)(C) (2001). The opt out clause only requires entities to make "reasonable efforts" to refrain from making marketing communications to the complaining individual. *Id.* at 514(e)(3)(iii). The individual has no recourse to prevent the spread of his or her personal information. *See id.*

175. 45 C.F.R. § 164.508(a)(3)(i) (2002).

ject to a valid authorization, but the standard is applied differently in each. In the former, information could be dispersed absent authorization if the entity were making a "marketing communication . . . concern[ing] products or services of nominal value."[176] The regulatory language suggests that the total value of the product or service must be nominal. By contrast, in the modified rule, the limitation concerns communications in the form of "promotional gift[s] of nominal value provided by the covered entity."[177] The nominal value here relates only to the sample provided, which may be an inexpensive sample of a very expensive product. Since the communication concerns a treatment alternative (suggested by the sample), entities are free to disclose enrollee information to business associates to generate the promotional sending under the guise of health care operations.[178] Here, unlike the demand-creating brochures that are excluded from the definition of marketing, demand management *is* coupled with incursions on disclosure privacy.[179] This increases vulnerability to exposure of private information since business associates, unless they are themselves covered entities, are not governed directly by the regulations.[180]

An individual may welcome a sample directly from the direct health care provider. That does not mean that the individual

176. 45 C.F.R. § 164.514(e)(2)(i)(B) (2001) (dovetailing with § 164.501(6)(v) of the definition of "health care operations").

177. 45 C.F.R. § 164.508(a)(3)(i)(B) (2002). In both the initial and modified versions of the final Rule, there was no limitation on subject matter. However, to meet the § 164.502(a) standard of dissemination, uses or disclosures must fit within an enumerated purpose, unless authorized. *See* 45 C.F.R. § 164.502(a) (2001) & (2002). But to avoid the authorization requirement that section 164.508 specifically allows, it would need to fit within the permissive structure – most notably, within the definition of health care operations. 45 C.F.R. § 164.502(a)(1)(ii) (2002). Health care operations is a natural fit. It includes activities aimed at reducing costs, which by implication would include the development of mass mailings of samples to encourage use of the cheapest costing products in accord with contracts with suppliers of the samples. It also permits contact with the individual for treatment alternatives, implying a health-related matter. 45 C.F.R. § 164.501 (2002). Dissemination of private health information for purposes of accomplishing the operations purposes requires no authorization; it is permissive. 45 C.F.R. § 164.502(a)(1)(ii) (2002).

178. *See* 45 C.F.R. § 164.502(e)(1)(i) (2002). Similar practices of inducing patients to switch to cheaper medications has been controvercial in the past. Scott, *supra* note 22, at 502.

179. *See* Sage, *supra* note 71, at 1788-89 (discussing information tools used to persuade).

180. *See* 45 C.F.R. § 160.102 (2002). Business associates fall outside the scope of the regulatory agency's authority as granted by Congress (unless they are also themselves statutorily-controlled entities independent of their business associate contracts). Therefore, the Rule is limited to requiring covered entities who disclose information to business associates to have written documentation of "satisfactory assurance that the business associate will appropriately safeguard the information." 45 C.F.R. § 164.502(e)(1)(i), (e)(2) (2002).

welcomes the spread of private health information in exchange for the gift.[181] By definition, the cost of the gift is very low to the providing entity. The cost to the individual might be greater than the gift is worth, given increased vulnerability to exposed privacy. Because the revised regulation focuses on the de minimis value of the gift sample rather than the total value of the product or service offered, the entity has an incentive to disseminate and aggregate private health information to facilitate its promotional gift giving. As there is no limit on the quantity of promotional mailings that may occur, an entity may seek to maximize its profit by multiple disclosures that result in multiple remunerated mailings without a charge of non-compliance with the privacy regulations.

Since the promotional gift falls outside the scope of requiring authorization (as long as the covered entity is the gift provider),[182] then there may be no requirement that an individual learn about any remuneration to the entity by the product manufacturers or service coordinators. The reason for the lack of knowledge is that the regulations seem to provide for remuneration notice within authorizations separate from the communication,[183] which are not required for promotional gifts.[184] This is consistent with the initial final Rule insofar as disclosure of some marketing is permissive.[185]

An entity that discloses private health information without prior authorization in order to make promotional gifts may then follow up by making recommendations to the individual to use those same products and services without the authorization or remuneration requirements attached to marketing communications.[186] The reason for this anomaly is that entity recommendations for alternative treatments and exclusive offerings of health-related products and services to

181. This reflects the double-headed issue of service versus exploitation. Schatz, *supra* note 66, at 687.

182. 45 C.F.R. § 164.508(a)(3)(i)(B) (2002).

183. *See* 45 C.F.R. § 164.508(3)(ii) (2002) ("If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved"). It is unclear whether a specific reference to remuneration must appear within the formal Notice. *See* 45 C.F.R. § 164.520(b)(1) (2002).

184. *See* 45 C.F.R. § 164.508(3)(i)(B) (2002) (stating authorization not required for de minimis promotional gifts).

185. *See* 45 C.F.R. § 164.501 (2001) (part (v) of the definition "health care operations") in conjunction with 45 C.F.R. § 164.514(e)(2)(i)(B) (2001), which negated the authorization requirement for the marketing of nominal valued goods and services and placed the activity within the purview of the permissive health care operations.

186. *See* 45 C.F.R. § 164.501(1) (2002) (parts (1)(i) and (1)(ii) of the definition of "marketing"); *see also* 45 C.F.R. § 164.501 (2002) (defining "health care operations") and (stating permissive disclosure is permitted if culminating in contact about a treatment alternative).

health plan enrollees falls outside the definition of marketing.[187] The modified final Rule provides that communications describing health-related products or services are not marketing if they are "available only to a health plan enrollee that add value to, but are not part of, a plan of benefits."[188] That means that a plan can offer a set of products or services at a cheaper price to enrollees, thereby adding value because individuals would not be eligible for the special price except for enrollment.

The activity would be subsumed within health care operations.[189] Therefore, no authorization would be required prior to disclosure of information that generated the communication, and no apparent notice regarding possible remuneration from the manufacturer or service coordinator to the entity would be required.[190] Interestingly, the new regulations appear to have abandoned the earlier version's requirement that individuals who are targeted be told about entity targeting strategies.[191] Instead, the communications appear to fall within the scope of health care operations[192] and would be subject only to requirements attached to those activities. Under both the initial and modified rules, permissive disclosures as part of health care

187. *See* 45 C.F.R. § 164.501 (2002) (parts (1)(i) and (1)(ii) of the definition of "marketing"). Communications are not considered marketing if they are about "health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits." *Id.*

188. *Id.*

189. *See* 45 C.F.R. § 164.501 (2002). "Health care operations" includes the ambiguous "related functions that do not include treatment" as well as contacting individuals about treatment alternatives. *Id.* Read together, the definition would allow for entities, within the permissive context of operations activities, to explore a means of reducing its costs by maintaining some uniformity of medication among enrollees, even if the product sample might not be the best health choice for the recipient enrollee.

190. *See* 45 C.F.R. § 164.508 (2002). A cautious covered entity might wish to guard against possible suits by seeking authorization from enrollees for the marketing strategies described. If the authorization is sought at the time of enrollment, it is likely that individuals will not be fully cognizant of the implications. How many people actually read entire documents – even those they are asked to sign? The "plain language" requirement, 45 C.F.R. § 164.508(c)(3) (2002), does not guarantee an understanding of what is being asked, particularly when combined with the presentation of other documents, and detached from the diagnosis or treatment of a health condition. This would be true unless section 164.520 were interpreted to require remuneration specifics.

191. *See* 45 C.F.R. § 164.514(e)(3)(ii) (2001).

192. *See* 45 C.F.R. § 164.501(2002). Falling outside of the definition of "marketing" is not why uses or disclosures may occur. Instead, they occur because they fall *within* the permissive provisions of health care operations. *See* 45 C.F.R. § 164.502(a) (2002).

operations threatens patient privacy and blurs the line between medicine and marketing.[193]

How do these changes affect the operations non-marketing marketing contacts between the covered entities and our hypothetical John Doe?

(ii). Application

Unlike the initial version of the final rule, which required notice of remuneration at the time operations marketing communication were made,[194] the modified version required but a single notice at the time an authorization was sought (which could have occurred in conjunction with other signed documents at the time of enrollment),[195] or possibly no notice at all.[196] Consequently, John might not know that the entity-sent product samples targeting him or the face-to-face counseling from a member of the entity (either in person or via door-to-door communication) could be motivated by entity gain rather than individual benefit. The focus on the nominal value of a sample conjoined with crossover between entity and individual benefit appears to increase the entities' desire to disseminate information for its own gain. In turn, this could increase John's vulnerability to privacy breaches despite the retention of the standard that uses or disclosures are limited to the minimum necessary.[197] Moreover, since modifications removed

193. *See* Scott, *supra* note 22, at 502-03 (noting the tension between industry and privacy advocates in striking the proper balance between patient interests and profit motive).

194. 45 C.F.R. § 164.514(e)(3)(i)(B) (2001).

195. Note the compounding allowances, 45 C.F.R. § 164.508(b)(3) (2002), and the absence of timing requirements in the implementation specifications of section 164.508(c).

196. Absent the need for authorization, John may receive no notice of any remuneration that the entity may have received from the supplier. *See* 45 C.F.R. § 164.508(a)(3) (2002). Notification of remuneration occurs within authorization documents. 45 C.F.R. § 164.508(a)(3)(ii) (2002). If no authorization is required for the marketing (as provided by § 164.508(a)(3)(i)(B) (2002)), then the individual will not receive remuneration information unless the entity voluntarily provides it. It is unclear the extent to which the notice document itself would require individuals to be specifically informed. It must contain sufficient information to put the individual "on notice" about the kind of dissemination that is permitted to occur in the absence of specific authorization. Required information includes a general description of disclosures in connection with operations, activities, and a description of "other purposes." 45 C.F.R. § 164.520(b)(1)(ii) (2002). However, there is no requirement that it be contained in a separate statement that would call attention to the permissive uses and disclosures. 45 C.F.R. § 164.520(b)(1)(iii) (2002). Thus, descriptions sufficiently detailed to provide the requisite notice are also likely to be sufficiently detailed to inhibit reading.

197. 45 C.F.R. § 164.502(b) (2002); 45 C.F.R. § 164.514(d)(1) (2002). The modified Rule includes an additional section regarding permissive use of a limited data set in conjunction with research, health information, or health care operations. 45 C.F.R. § 164.514(e)(1), (3) (2002). It may find its greatest application in the re-

the requirement of a remuneration notice with each mail out, John might not realize that the product and service information he received was remunerated. Nor would it trigger an understanding of a distinction between products and services for his treatment benefit, and those marketed not primarily for his benefit. The blurring of the treatment/marketing line suggests an inability to recognize what disclosures were permissive, over which John had no control, and those made pursuant to an authorization, which John could potentially revoke.[198]

2. *Participants' Ability to Self-Protect*

Suppose John found it embarrassing to receive the solicitations and greatly upsetting that his private affairs concerning his health conditions were passed on to others within or outside the communicating entity. Could John exercise some privacy right to limit the communication or dissemination?

One of the hallmarks of privacy is that a person has control over the dissemination of information about him or herself.[199] Thus, notwithstanding the grant of permission by the Rule for entities to disclose protected health information to their business associates for the purpose of advertising products and services of potential benefit to targeted individuals, no violation of privacy occurs if John may limit the disclosures himself.

If John could exercise opt out rights, he could exercise control over his own affairs and thereby preserve his privacy. Apparently in accord with this principle, the initial final rule mandated certain opt out rights in order for a marketing communication to retain its status as a health care operation.[200] Each marketing communication, unless of a general nature with broad based distribution, required instructions on how to opt out.[201] But the opting out provision was limited to cur-

search context, which needed some of the data removed when de-identified. *See* INST. FOR HEALTH CARE RESEARCH AND POLICY, GEORGETOWN UNIVERSITY, HEALTH PRIVACY PROJECT, COMMENTS ON PROPOSED MODIFICATIONS TO FEDERAL STANDARDS FOR PRIVACY ON INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION 18 (2002), *available at* http://www.healthprivacy.org (last visited Dec. 6, 2002). It is unclear how the use of limited data sets could affect health care operations. Its use is not mandatory, but rather is permissive. 45 C.F.R. § 164.514(e)(3) (2002). As applied to operational activities, the failure to exclude some potential re-identification data from the data set presents problematic privacy issues. *See* INST. FOR HEALTH CARE RESEARCH AND POL'Y, *supra* note 197.

198. An individual has a right to revoke an authorization if the entity has not acted in reliance. 45 C.F.R. § 164.508(b)(5) (2002).

199. *See* INNESS, *supra* note 27, at 57.

200. *See* 45 C.F.R. § 164.501 (2001) (part (6)(v) of the definition of "health care operations"); 45 C.F.R. § 164.514(e)(2)(C), (3)(i)(C) (2001).

201. 45 C.F.R. § 164.514(e)(3)(i)(C) (2001).

tailing future communications.[202] Once John had expressed his interest in being free of the harassing solicitations, the entity was only required to make "reasonable efforts to ensure that individuals who decide[d] to opt out of receiving future marketing communications . . ., [we]re not sent such communications."[203] This was analogous to the privacy rights preserved by the common law intrusion upon seclusion tort[204] and did not address concerns relating to the disclosure aspect of his privacy interests. Thus, while John's embarrassment in receiving communications may have been alleviated, his concern over the information flow was not addressed.

Under the modified rule, John's only real hope is to read carefully and refuse to grant authorization, or attempt to trace communications to authorizations and seek to revoke them. There is no opt-out provision that could curtail the communications.

Are there any other rights that John could exercise to limit or interrupt the flow of his private health information where it concerns marketing?

John does have a right to request that entities limit uses and disclosures of his private health information.[205] The Rule's choice of the word "request" symbolizes that power and control rest in the holder, and not in John, the person whose private matters are revealed or withheld by the holding entity. As the word choice implies, John's request need not be honored.[206] This may be true even if a covered entity has agreed to restrict some use or disclosure at John's request. The entity is not bound to comply if the disclosures are, under certain circumstances, legally permissible or required.[207] The agreement

202. *Id.* at 514(e)(3)(iii).

203. *Id.*

204. Makdisi, *supra* note 30, at 989.

205. 45 C.F.R. § 164.522(a)(1) (2001) & (2002). This right must also be stated in the notice. 45 C.F.R. § 164.520(b)(iv)(A) (2001) & (2002).

206. 45 C.F.R. § 164.522(a)(1)(ii) (2001) & (2002).

207. 45 C.F.R. § 164.522(a)(1)(v) (2001) & (2002). Even if an entity agrees to block uses or disclosures, the agreement is ineffective "to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(i), 164.510(a) or 164.512." Section 164.502(a)(2)(i) refers to an individual's right of access to his or her record and to the individual's right to discover to whom the entity has made disclosures about the individual. Section 164.524 denies an individual access to, *inter alia*, psychotherapy notes, litigation disclosures, certain clinical disclosures, information from someone other than a health care provider that was received under a confidentiality agreement with the person supplying the information, and when disclosure to the individual in specified contexts would result in substantial harm. Section 164.528 denies an individual a right to discover what information has been disclosed (and to whom) provided consent was granted or was not required, such as when information is exchanged between two health care providers (referring to § 164.502 and § 164.506); provided disclosure had been authorized (referring to § 164.502); or provided that the individual had a prior opportunity (oral notification and response suffices) to restrict directory entries and information

with John would be void, for example, if the Food and Drug Administration were tracking a product prescribed to John,[208] or if John were at risk of contracting or spreading a communicable disease for which an alert had been issued to the entity.[209]

Disclosures made contrary to a private agreement between John and an entity would be quite damaging to John's subjective view of his privacy. This would be particularly true if John were left in the dark regarding the potential disclosures[210] or if John had chosen to seek medical care premised on the belief that his private health information would be held in strictest confidence based on the agreement.[211] Nevertheless, the privacy model is not the subjective, but objective view as measured by what would be a collective desire. The collective desire might regard such disclosures as reasonable or even necessary to the framework of general social life. Therefore, privacy in that global sense might be adequately protected under the discussed limitations, which do not permit contra-agreement disclosures for marketing purposes.

---

flow to those involved with the individual's care or payment (referring to § 164.510). The individual also may not curtail legally required disclosures including instances of abuse, neglect or domestic violence; disclosures pertinent to a judicial or administrative proceeding; or those made to law enforcement for some purposes. 45 C.F.R. § 164.512. It is apparent that an individual may not limit such disclosures, notwithstanding any restriction agreements with covered entities.

208. *See* 45 C.F.R. § 164.512(b)(1)(iii)(B) (2001) & (2002).

209. *See* 45 C.F.R. § 164.512(b)(1)(iv) (2001) & (2002).

210. This would depend on how well he reads and understands the notice provisions, and whether the notice contains information relevant to the voidability of restriction agreements. There appears to be no requirement that disclosures made contrary to the restriction agreement be disclosed to the individual with whom the agreement is made. *See* 45 C.F.R. § 164.522 (2002). It is unclear whether the notice must include this information. The notice must contain "[a] description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written consent or authorization." 45 C.F.R. § 164.520(b)(1)(ii)(B) (2001) & (2002) (except that in the modified version, the word "consent" is dropped since consent is no longer required for any uses or disclosures). Even if the examples above fall within "other purposes," would the supplied description sufficiently notify John, particularly if the notice were provided two or three years earlier, at a time that John had no knowledge of his current condition?

211. Seeking care because individuals had trust in entity maintenance of confidentiality is an important concern of Congress in developing the Rule. *See* Preamble, *supra* note 10. An additional privacy issue regards information placed in the files of an individual by one other than a provider. If there is a confidentiality agreement between the informant and the entity and the informant's identity could be discerned, then the individual about whom the information was about could not access it. He might not even be aware of its existence. Nor would he have the opportunity to challenge its truth. *See* 45 C.F.R. § 164.524(a)(2)(v) (2001) & (2002).

The above discussion suggests that there is no meaningful mechanism by which an individual has control over the dissemination of his or her private information.[212] If John cannot control the dissemination, could he at least follow the path of dissemination to discover the extent of his vulnerability or to preserve any remedy rights in the event that inappropriate disclosure has occurred? Under the Rule, John has a right to receive an accounting of disclosures.[213] This is another one of the specified individual rights of which individuals must be informed by the notice.[214] If one examines the accounting standard as defined by section 164.528, the right appears to be broadly inclusive since it encompasses disclosures made during the six years prior to the request.[215] Note, however, that the accounting right does not include the right to trace the path of intra-entity "uses."[216] This absence may be unimportant if the standards governing uses do not violate privacy as determined by the collective desire. Of real import, on the other hand, are the exceptions to the standard.

Three exceptions severely curtail John's accounting rights. The first excepts accounting of disclosures made for purposes of treatment, payment, and operations.[217] Since entities may share information with business associates for health care operations, including marketing as discussed above, John has no means of learning about the extent of sharing or the identities of the recipients.[218] Under the modified rule, John's rights are similarly curtailed by the inability to be informed about disclosures pursuant to authorization.[219] Despite the absence of such need on its face (since John must have authorized the disclosures), the authorization may have been timed such that John could not recognize how the authorization translated into specific disclosures or communications.[220] Finally, the right to an accounting does not include disclosure of limited data sets, despite their

212. Inness points out that privacy is not lost merely because of our desire to keep the information secret. It may only be lost if the content of the information itself is truly private. INNESS, *supra* note 27, at 58-59. With respect to health information, there is no dispute that the information is the "secret" type over which one should have an expectation of privacy, as acknowledged in the Rule itself. *See* Preamble, *supra* note 10 and definitions. 45 C.F.R. § 164.501 (2001) (defining "individually identifiable health information").

213. 45 C.F.R. § 164.520(b)(1)(iv)(E) (2001) & (2002).

214. *Id.* Another specified individual right just discussed was the right to request restrictions on certain uses and disclosures.

215. 45 C.F.R. § 164.528(a)(1) (2001) & (2002).

216. *Id.* The standard refers to disclosures and not to uses. *Id.*

217. 45 C.F.R. § 164.528(a)(1)(i) (2001) & (2002).

218. *See* 45 C.F.R. § 164.520 (2002), which does not require disclosure of the extent or identities of information recipients. *See also* note 122.

219. 45 C.F.R. § 164.528(a)(1)(iv) (2002). This was not an exception in the final rule. 45 C.F.R. § 164.528(a)(1) (2001).

220. *See* discussion *supra* notes 115-120 and accompanying text.

peculiar problem of potential re-identification.[221] In short, John's ability to track the dissemination of his private health information is extremely limited. This may even be compounded if John were not the named "insured," because he may not have received a notice of entity sharing policies unless he were savvy enough to have requested the information on his own.[222]

If John cannot trace the path of dissemination, may he find a source of relief that his private information has a final destination in the entity's business associates? No Business associates may use or disclose private health information pursuant to a contract with a covered entity[223] "if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information."[224]

Suppose that, despite the obstacles, John were successful at determining that an improper disclosure had occurred.[225] What would be John's remedy? Possibly none. Any right enforceable under the common law might be preempted,[226] and John has no private right of action under the Rule. Instead, penalties are assessed by the HHS Secretary.[227] There are no penalties for negligent disclosures if corrected within thirty days after the negligence is or should have been discovered.[228] Correction may be accomplished by taking reasonable steps to cure, terminating contracts with associates who do not cure material breaches, or, if termination were not feasible, reporting the problem to the Secretary.[229]

Since the remedy structure is unsatisfactory, could John end all the information flow by simply dis-enrolling from a plan and enrolling somewhere else? Such evasive action would likely be unsuccessful. Private health information may be used and disclosed by covered entities for health care operations, and those entities may share informa-

221. 45 C.F.R. § 164.528(a)(1)(viii) (2002). *See* discussion *supra* note 122 regarding the impact of limited data sets. Data sets were not part of the initial final Rule.
222. *See* 45 C.F.R. § 164.520(c)(1)(iii) (2001) & (2002). Only the named insured must be provided notice absent specific request. *Id.*
223. 45 C.F.R. § 164.504(e)(2) (2002).
224. 45 C.F.R. § 164.502(e)(1)(i) (2002).
225. History tells us that improper disclosures did not necessarily result from computer transgressions; some of the worst infractions were due to human error. *See* Davis, *supra* note 130, at 539. This augments the problems of lack of control over business associates.
226. 42 U.S.C. 1320d-7 (1996). Preemption promises to be a huge issue as state privacy laws are interpreted in conjunction with the Rule. *See* Starr, *supra* note 9, at 201.
227. HIPPAA, § 262 (codified as 42 U.S.C. § 1320d-7; 45 C.F.R. 160.203). The Secretary, in turn, has delegated the imposition of monetary penalties to the Director of the Office for Civil Rights. 65 Fed. Reg. 82,381 (Dec. 28, 2000), *available at* http://www.aspe.hhs.gov/admnsimp/final/PvcFR.htm (last visited June 1, 2001).
228. HIPAA, § 262 (administrative simplification).
229. 45 C.F.R. § 164.504(e)(1)(ii) (2002).

tion with other entities with relationships with the individual, either currently *or* in the past.[230] This means that an individual is unable to eliminate undesired transmission of private information even if he or she switches to a new provider or health plan schema. While it may be desirable for treatment and diagnosis purposes, it does not seen part of the *quid pro quo* when it concerns operational activities of the entity, particularly since all the disclosures may occur without even the consent of the individual.[231] The former regulations required an individual to at least consent to provider disclosures for treatment, payment, and operations.[232] In the revised regulations, consent is not required.[233]

Moreover, uses and disclosures may continue to ever larger groups of business associates of business associates as long as each, in turn, includes a disclosure provision in their contract that also provides "reasonable assurances" of adhering to the Rule.[234] With each use or disclosure, the private information becomes increasingly more vulnerable to negligent or intentional unpermitted disclosures or other unauthorized retrievals of the information. To curtail the increasing exposure, individuals should be provided information with communications that enables the individual to have some ability to trace and limit the information flow, and be granted an option to opt out of the benefit specific to all practices an unsophisticated consumer would consider marketing. These primarily benefit the entity rather than the individual's health care that was the *quid pro quo* in the exchange resulting in the loss of control over private information. To permit less fails to fulfill the collective desire and thereby fails to protect privacy.

V. CONCLUSION

Payment purposes have practicalities having to do with fair exchanges and with governmental purposes of fraud prevention and system efficiency. Treatment purposes have lingering paternalism. Doctors still know best. In order to properly diagnose and treat, information should not be withheld. This is the essential trust relationship between a learned professional and lay client. In both instances, despite any worrisome consent issues that linger, the *quid pro quo* between lost privacy and benefit gained from entry into the organized health care mini-society appears to protect privacy to the extent practical and has the semblance of collective desire as measured by objective reason.

230. 45 C.F.R. § 164.506(c)(1), (4) (2002) (emphasis added).
231. 45 C.F.R. § 164.506(b) (2002).
232. 45 C.F.R. § 164.506(a) (2001) (stating provider needed to obtain consent).
233. 45 C.F.R. § 164.506(b) (2002).
234. 45 C.F.R. § 164.504(e)(2), (4)(ii)(B)(1) (2002).

Operations purposes do not appear to reflect the objective reason necessary for a collective desire. Need as defined by Congress includes the reduction of governmental cost in running federal health care programs as well as increasing efficiency. Arguably, encouraging participants to use cheaper treatments by providing samples and treatment recommendations comporting with favorable entity-supplier contracts suggests condoning unfettered dissemination to accomplish that purpose.[235] On the surface, then, tort-like balancing may not appear to favor disclosure limitations, even in the context of commercial marketing. However, that simplistic formula fails to consider other important balancing factors. The absence of meaningful choice regarding dissemination practices, an entity's driving profit motive as the real reason behind its practices,[236] and a need for the development of trust suggest that the broad disclosure practices permitted under the Rule do not provide an objective measure of reasonableness,[237] particularly in the context of marketing disguised as health care operations.

If marketing continues to be disguised under operational activities, accounting rights should be enlarged to re-include disclosures made pursuant to authorization. Consumer confusion and attenuation between authorizations and activity imply this need. This is especially true since notices that provide boilerplate laundry lists may not be helpful to increase a participant's understanding of actual disclosure practices, which may include remunerated activity. Each communication that an unsophisticated participant would consider marketing should include the initial final rule's requirements of remunerated notice at the time of a marketing communication as well as an explanation of how to pursue opt-out rights.

The Rule should be adjusted to restrict disclosures for marketing purposes that are disguised as health care operations. Those practices essential for entities as a whole should remain in the current realm of permissive disclosures. Essential operational features that vary among entities should be separately addressed in order that the marketplace dictate which entities should survive. If the collective desire would place a higher value on privacy over specific benefits gained by varied entities, then the marketplace will reflect the nature of the services in exchange for lost privacy.

Finally, uses and disclosures in the context of all practices that consumers would deem "marketing," regardless of the technical defini-

235. Physicians may even have a duty to reduce costs. Sage, *supra* note 71, at 1753.

236. Clark C. Havighurst, *Health Care as a (Big) Business: The Antitrust Response,* 26 J. HEALTH POLITICS, POL'Y & LAW 939 (2001); *see also* Sidney D. Watson, *Commercialization of Medicaid,* 45 ST. LOUIS U. L.J. 53, 61 (2001) (discussing how Medicaid is dominated by for-profit entities).

237. Gostin, *supra* note 9, at 34-35.

tion of that practice as a "health care operation," should have a meaningful opt-in[238] or, at a minimum, an opt-out rider. The opt-out provision should be more liberal than what was in the initial final rule. The opt-out provisions should all be converted from harassment opt-out to disclosure opt-out. In addition, the means by which a person should be able to opt out should be easy to find and easy to accomplish. Only then may a person's privacy be protected.

238. *See* James Molenaar, *supra* note 12. Unless authorization signaling the opt-in provision is provided in a manner designed to provide the consumer with a full understanding of how his or her private information is disseminated, the option's helpfulness would be minimal.