THE INADEQUACY OF HIPAA'S PRIVACY RULE: THE PLAIN LANGUAGE NOTICE OF PRIVACY PRACTICES AND PATIENT UNDERSTANDING

*MARIE C. POLLIO**

INTRODUCTION

Polls have shown that the public is significantly concerned about the lack of privacy of medical information.[1] Lack of confidence in the security of health information leads patients to "lie or withhold information from their providers; pay out-of-pocket for care; see multiple providers to avoid the creation of a consolidated record; or sometimes avoid care altogether . . . behavior[s] [that] can compromise both individual care and public health initiatives."[2] As more and more data is stored and managed electronically, concern over the security of the data and the lack of confidentiality of individuals' health information has grown.[3] Inad-

* Associate, Shipman and Goodwin LLP; Executive Articles Editor, *NYU Annual Survey of American Law* 2003–04; J.D. *cum laude*, New York University School of Law 2004; M.Ed. University of Vermont; B.A. *magna cum laude*, New York University. Many thanks to Professor Sylvia Law, Ms. Pietrina Scaraglino, and the staff of the *NYU Annual Survey of American Law* for their thoughtful assistance in the preparation of this article. This note is dedicated to Scott and Zachary Halstead. All opinions expressed herein are solely the author's.

1. Surveys by the California HealthCare Foundation and Louis Harris & Associates indicate that 20% of Americans believe their medical information has been improperly disclosed and a Gallup survey found that more than 60% are concerned that their health information will be made available without their consent. HEALTH PRIVACY PROJECT, HEALTH PRIVACY POLLING DATA 1–2, *available at* http://www.healthprivacy.org/usr_doc/PollingData9012.pdf (last modified Sept. 2001).

2. HEALTH PRIVACY PROJECT, BEST PRINCIPLES FOR HEALTH PRIVACY 3 (1999), *available at* http://www.healthprivacy.org/usr_doc/33807.pdf [hereinafter HPP BEST PRINCIPLES]; *see also* 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) ("Patients may not fully disclose all medical problems in fear of an unforeseen record disclosure.").

3. Patricia I. Carter, *Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age"?*, 25 WM. MITCHELL L. REV. 223, 230 (1999); HPP BEST PRINCIPLES, *supra* note 2, at 3; Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 617–18 (2002).

equate protections can lead to unauthorized disclosures of health information that "may subject individuals to social stigma and discrimination by insurance companies, health care professionals and institutions, and employers."[4] Although technology can provide some security protections, such measures are not foolproof; additional legal protections are required.[5]

While the protection of health information is an important value, there are also some very legitimate reasons to access medical information, such as for public health purposes, research, and to improve care.[6] The tension between the two goals of privacy protection and access for legitimate reasons forms the basis of the debate surrounding the creation of health privacy regulation.[7]

In light of the ease with which health information could be shared with a broad audience, the need for a uniform national policy of medical information privacy became clear.[8] In April 2001, the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) took effect. The Privacy Rule, promulgated by the United States Department of Health and Human Services (HHS) under authority granted by the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[9] constitutes the first "systematic national privacy protections of health information."[10] Al-

4. Lawrence O. Gostin et al., *Balancing Communal Goods and Personal Privacy under a National Health Information Privacy Rule*, 46 ST. LOUIS U. L.J. 5, 10 (2002). For examples of the types of unauthorized disclosures made and their effects, see HEALTH PRIVACY PROJECT, MEDICAL PRIVACY STORIES, *available at* http://www.healthprivacy.org/usr_doc/privacystories814.pdf (last updated Aug. 14, 2002).

5. Carter, *supra* note 3, at 235–36.

6. *See, e.g.*, HPP BEST PRINCIPLES, *supra* note 2, at 9–10.

7. *See* Gostin, *supra* note 4.

8. As early as 1983, commentators argued that the legal protections of health information privacy were inadequate to protect individuals' most sensitive information. *See, e.g.*, Ellen Klugman, *Toward a Uniform Right to Medical Records: A Proposal for a Model Patient Access and Information Practices Statute*, 30 UCLA L. REV. 1349, 1376–77 (1983) (arguing that the hodgepodge of common law and state legislative efforts to secure health information privacy is inadequate because organizations that collect and process health information operate, in many cases, on a national scale).

9. Pub. L. No. 104-191, 110 Stat. 1936 (1997) (codified in scattered sections of 26, 29, 42 U.S.C.).

10. Gostin, *supra* note 4, at 5.

though the Privacy Rule underwent some modification in 2002,[11] compliance with it was expected as of April 14, 2003.[12]

The final version of the HIPAA Privacy Rule relies on an "enhanced" Notice of Privacy Practices (NPP) as the tool to actively involve patients in how their health information is used and disclosed. This reliance presumes that patients understand the notices that they receive from their health plans and health care providers. HHS, however, has made it clear that it is not the providers' responsibility to ensure that patients actually understand or even read the notices given to them. HHS merely requires that the NPP be written in plain language. In light of experiences with plain language requirements in other settings, common experiences with informed consent in the medical field, and theories of cognitive psychology, it is unlikely that patients will actually comprehend the notices. This is problematic because HHS has made the protection of patient rights largely dependent on patient involvement.

In this article, I argue that the Privacy Rule is internally inconsistent because it relies on disclosure to individuals as the primary mechanism for engaging individuals in controlling their health information, yet expressly requires nothing more than that the disclosure be written in plain language. With no detailed guidance, a plain language requirement does not ensure understanding. Additionally, the amount of information required to be included in the notice might lead to information overload and an inability to comprehend or attend to what is being presented. Finally, by crafting the notice to include only permissible uses and disclosures, HHS presumes that patients have a basic understanding of all the possible uses of health information, can differentiate permissible from impermissible uses, and therefore can know when their rights have been violated.

Part I discusses the background of HIPAA and the various regulations promulgated thereunder, including a detailed overview of the Privacy Rule, with particular emphasis on the requirements found in the Notice of Privacy Practices. Part II discusses the debate surrounding plain language requirements. Part III analyzes why the mere requirement of a plain language disclosure is inadequate to achieve the purposes intended by the NPP, in light of the

11. Standards for the Privacy of Individually Identifiable Health Information; Final Rule, 67 Fed. Reg. 53,182, 53,183 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160, 164) [hereinafter Privacy Rule]. Unless otherwise indicated, the term Privacy Rule will be used herein to denote the combined regulations of the 2000 and 2002 Rule.

12. Department of Health and Human Services, 45 C.F.R. § 164.534 (2004).

lessons learned from informed consent, people's inability to attend to too much information, and people's tendency to comprehend through inference. Finally, Part IV recommends some improvements to the NPP requirement so that it may achieve its goals.

I.
HIPAA OVERVIEW

This section is designed to provide the context of the privacy regulation by examining the organic statute and companion regulations. Included is a description of the history, purpose, key provisions, and major critiques of the Privacy Rule. I begin with an overview of the Health Insurance Portability and Accountability Act of 1996, the Privacy Rule's organic statute.

A. The Health Insurance Portability and Accountability Act of 1996

In August 1996, Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[13] The act was intended to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, [and] to simplify the administration of health insurance . . . ."[14]

HIPAA arose from Congress' concern over the number of Americans facing "job-lock," a phenomenon in which people who received medical insurance from their employer felt constrained to remain in that job out of fear that waiting periods and pre-existing condition exclusions would lead to a denial of coverage in a new job that offered health insurance.[15] With over 62% of Americans covered by employment-based health insurance, the risk of job-lock was widespread.[16] HIPAA alleviates the problem by requiring group health plans to credit previously carried insurance as coverage for a pre-existing condition,[17] and prohibiting group health plans from excluding coverage for individuals based on their health status.[18]

13. Pub. L. No. 104-191, 110 Stat. 1936 (1997) (codified in scattered sections of 26, 29, 42 U.S.C.).

14. H.R. REP. NO. 104-496, at 1 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1865, 1865.

15. *Id.* at 68–69, *reprinted in* 1996 U.S.C.C.A.N. at 1868.

16. *Id.* at 74, *reprinted in* 1996 U.S.C.C.A.N. at 1873.

17. *Id.*, *reprinted in* 1996 U.S.C.C.A.N. at 1874.

18. *Id.* at 76, *reprinted in* 1996 U.S.C.C.A.N. at 1876.

Congress was also concerned about the rising cost of health care, which was exacerbated by two major problems: fraud and abuse of health care services, and the administrative burden caused by medical paperwork.[19] To combat fraud and abuse of the health insurance system, HIPAA imposes a strict anti-fraud provision, through which fraud investigations are coordinated through HHS and the Department of Justice (DOJ). HIPAA allocates funds and mandates that HHS oversee and audit for fraud and abuse.[20]

To reduce the burden of medical paperwork and create savings in the health care industry, Title II of HIPAA provides for administrative simplification by establishing a health information network. Specifically, uniform medical transaction codes are mandated whenever electronic billing and information transmission occurs.[21] Without such uniformity across health care institutions, modernization of information technology is more difficult and opportunities for cost savings are lost.[22]

Recognizing that consolidating all health information in one place or in one format raises concerns over the confidentiality and privacy of the information, HIPAA also directs the HHS Secretary to "adopt standards relating to the privacy of individually identifiable health information concerning the rights of individuals who are the subject of such information, the procedures for exercising such rights, and the authorized uses and disclosures of such information."[23] As part of the enforcement of such standards, Congress created the offense of "wrongful disclosure of individually identifi-

19. *Id.* at 69, *reprinted in* 1996 U.S.C.C.A.N. at 1869.

20. *See* HIPAA, Pub. L. No. 104-191, § 201, 110 Stat. 1936, 1992 (1997) (codified at 42 U.S.C. § 1320a-7c (2000)); *see also* Colleen M. Faddick, *Health Care Fraud and Abuse: New Weapons, New Penalties, and New Fears for Providers Created by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")*, 6 ANNALS HEALTH L. 77, 79–86 (1997). The fraud enforcement initiatives have "resulted in a greater number of investigations, prosecutions, civil enforcement proceedings, and recoveries." *Health Care Fraud and Abuse: Enforcement & Compliance*, HEALTH L. & BUS. (BNA), No. 2600, § 2600.01, at D. The funding and coordination of effort between DOJ and HHS have enabled enforcers to target white-collar crime in the health care industry. R. Kenneth Gordon, *OIG Steps up Fraud Enforcement: What that Means for the Health Care Industry*, 65 TEX. B.J. 837 (2002).

21. § 261, 110 Stat. at 2024–25 (codified at 42 U.S.C. § 1320d-2 (2000)).

22. H.R. REP. NO. 104-496 at 70, *reprinted in* 1996 U.S.C.C.A.N. at 1869.

23. *Id.* at 100, *reprinted in* 1996 U.S.C.C.A.N. at 1900. Similar language is found in the House Conference Report No. 104-736 at 265 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1990, 2078 ("The Secretary would be required to establish standards regarding the privacy of individually identifiable health information that is in the health information network.").

able health information" in order to "reflect[ ] the Committee's concern that an individual's privacy be protected."[24]

In addition, HIPAA amends the tax code to make it easier for Americans to save for medical expenses by, among other things, creating a tax-deductible medical savings account.[25]

While the statute was being passed, most of the congressional debate centered on concerns about the tax-related provisions and the inclusion of provisions that weaken the anti-fraud initiatives.[26] The congressional reports do not include protection of privacy as a purpose of HIPAA,[27] and the discussion of privacy is limited to the following:

> Protecting the privacy of individuals is paramount. However, the Committee recognizes that certain uses of individually identifiable information are appropriate, and do not compromise the privacy of an individual. Examples of such use of information include the transfer of information when making referrals from primary care to specialty care, and the transfer of information from a health plan to an organization for the sole purpose of conducting health care-related research. As health care plans and providers continue to focus on outcomes, research and innovation, it is important that the exchange and aggregate use of health care research be allowed.[28]

When President Clinton signed the bill into law, he focused on the portability of health insurance and on the requirement that health insurers renew insurance policies, telling anecdotal stories

24. *Id.* at 103, *reprinted in* 1996 U.S.C.C.A.N. at 1903.

25. § 301, 110 Stat. at 2037 (codified at 26 U.S.C. § 220); *see* Craig M. Stephens, *The Health Insurance Portability and Accountability Act: Favorable Tax Treatment for Medical Savings Accounts*, 20 AM. J. TRIAL ADVOC. 457 (1997). Reviews of the program have been mixed. *Compare* Regina T. Jefferson, *Medical Savings Accounts: Windfalls for the Healthy, Wealthy & Wise*, 48 CATH. U. L. REV. 685, 687, 704–12 (1999) (arguing that despite HIPAA's goal of "making health care more available to the general public, . . . [it] actually widened the gap between those who can afford adequate health care and those who cannot," because the medical savings account disproportionately benefits the wealthy, the healthy and the more informed health care consumer), *with* Greg Scandlen, *MSAs Can be a Windfall for the Rest of Us, Too*, 49 CATH. U. L. REV. 679, 679, 683–90 (2000) (arguing that when compared to other health care programs, medical savings accounts (MSAs) "have remarkable benefits for people of modest means and average, or less-than-average, health status").

26. *See* H.R. REP. NO. 104-496, at 279–84, *reprinted in* 1996 U.S.C.C.A.N. at 1984–89.

27. *See* H.R. CONF. REP. NO. 104-736, at 177, *reprinted in* 1996 U.S.C.C.A.N. at 1990; H.R. REP. 104-496, at 67, *reprinted in* 1996 U.S.C.C.A.N. at 1866.

28. H.R. REP. 104-496, at 100, *reprinted in* 1996 U.S.C.C.A.N. at 1900.

about people who lost their health insurance because of pre-existing conditions.[29] Clinton mentioned the privacy provision as part of a list of reforms that would "strengthen other aspects of our health care system."[30]

B. Administrative Simplification

The purpose of administrative simplification is to "improve the Medicare 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."[31] Specifically, administrative simplification requires the development of standards for electronic transactions, the establishment of a unique health identifier for each individual, employer, health plan and health care provider, the establishment of a uniform system of coding health data, and the adoption of standards for the security of health information, including an electronic signature system.[32]

To achieve administrative simplification, Congress required HHS to promulgate regulations covering security and electronic signatures, electronic data interchange (EDI), including transaction code sets and unique identifiers,[33] and if Congress failed to act on privacy—which it did[34]—then on privacy as well.[35] The security regulations establish "national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information" from threats posed by "improper access to stored information [and] interception during electronic transmission of the information."[36] The EDI regulations call for standardization in the processing and formatting of electronic transactions between health care providers, health plans and health care clearinghouses. The underlying goal is to "lessen the time and costs associated with receiving, processing, and storing documents[,] eliminate inefficiencies[,] and streamline processing tasks, which

29. Statement by President William J. Clinton upon signing H.R. 3103, 32 WKLY. COMP. PRES. DOC. 1480 (Aug. 26, 1996), *reprinted in* 1996 U.S.C.C.A.N. 2163.

30. *Id.* at 1480, *reprinted in* 1996 U.S.C.C.A.N. at 2163–64.

31. HIPAA, Pub. L. No. 104-191, § 261, 110 Stat. 1936, 2021 (1997) (codified at 42 U.S.C. § 1320d-2).

32. § 1173, 110 Stat. at 2024–26 (codified at 42 U.S.C. § 1320d-2).

33. *Id.*

34. Privacy Rule, 67 Fed. Reg. 53,182, 53,182 (Aug. 14, 2002).

35. § 264, 110 Stat. 2033–34 (codified at 42 U.S.C. § 1320d-2).

36. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164).

can in turn result in less administrative burden, lower operating costs, and improved overall data quality."[37]

HIPAA's unique identifier requirement calls for the assignment of a unique code to all health care providers, individuals, and employers.[38] Final rules have been published which adopt a National Employer Identification standard, basically adopting the employer identification number already in place for tax purposes and requiring the use of the number in all cases in which employers are involved in health care transactions.[39] Rules have been published concerning the adoption of a similar identifier for health care providers.[40] More controversial, however, is HIPAA's requirement of a unique identifier, similar to a social security number, for individuals. Proposed rules had not been established by November 2004, as disagreement over the wisdom of such a change stalled progress. On the one hand, a unique identifier simplifies the provision of health care from a patient's perspective, because a provider can access dispersed information through the use of one number. On the other hand, this greater access raises concerns about the potential for abuse and misuse.[41]

The statute also makes "recommendations with respect to privacy of certain health information."[42] This requires that HHS, after consulting with the Attorney General and the National Committee on Vital and Health Statistics, submit detailed recommendations to Congress on standards with respect to privacy, including rights that an individual should have, procedures for exercising such rights, and the uses and disclosures that should be authorized or required.[43] HIPAA requires Congress to pass legislation with respect to privacy by August 1999 and if Congress failed to do so, then HHS was directed to promulgate regulations by February 2000.[44]

37. Health Insurance Reform: Modifications to Electronic Data Transaction and Code Sets, 68 Fed. Reg. 8,381, 8,381 (Feb. 20, 2003) (codified at 45 C.F.R. § 162).

38. § 1173(b)(1), 110 Stat. at 2025 (codified at 42 U.S.C. § 1320d-2(b)(1)).

39. Health Insurance Reform: Standard Unique Employer Identifier, 67 Fed. Reg. 38,009 (May 31, 2002) (codified at 45 C.F.R. pts. 160, 162). *See also* Anthony C. Colletti & Tracey Sorens Pachman, *HIPAA: An Overview*, 13 HEALTH LAW. 14, 16–17 (2000).

40. HIPAA Administrative Simplification: Standard Unique Identifier for Health Care Providers, 69 Fed. Reg. 3,434 (Jan. 23, 2004).

41. *Id.* at 17.

42. § 264, 110 Stat. 2033–34 (codified at 42 U.S.C. § 1320d-2).

43. *Id.*

44. *Id.*

C. The Privacy Regulations

1. History

HIPAA required Congress to establish standards for the protection of privacy of health information by 1999.[45] Despite much debate, Congress was unable to agree on privacy standards. As a result, HHS promulgated regulations, known collectively as the Privacy Rule, which, after more than 52,000 public comments,[46] became final under the Clinton administration in December 2000. HHS continued to receive unsolicited comments regarding the "confusion and misunderstanding about how the Privacy Rule will operate [and] the complexity of the Privacy Rule."[47] HHS reopened comment on the Privacy Rule "[i]n response to these communications and to ensure that the provisions of the Privacy Rule would protect patients' privacy without creating unanticipated consequences that might harm patients' access to health care or quality of health care."[48]

Three major concerns were voiced. First, and most importantly, the health care industry was concerned with the consent requirement, which mandated patient consent before health information could be disclosed.[49] Many argued that the provision of health care would be impeded by the need to gather consents before treatment.[50] For example, when a specialist was needed, the specialist could not be consulted without receiving prior consent from the patient, and prescriptions could not be telephoned into pharmacies unless the patient had given advance written consent to the pharmacy.[51] Second, the industry was very concerned about the cost of implementation.[52] The third major concern was that inadvertent disclosures—which occur, for instance, when a receptionist phones in a prescription and is overheard by those in the waiting room—would result in violations.[53]

In March 2002, the Bush administration announced proposed modifications to the 2000 "final" privacy regulations, which, among other things, made pre-treatment consent optional and permitted

45. For a summary of the statutory history of the enactment of the Privacy Regulations see Privacy Rule, 67 Fed. Reg. 53,182, 53,182 (Aug. 14, 2002).

46. *Id.*

47. *Id.* at 53,183.

48. *Id.*

49. *See id.* at 53,209.

50. *Id.*

51. *Id.*

52. *See id.* at 53,255.

53. *Id.* at 53,193.

incidental disclosures.[54] HHS received more than 11,400 comments in the thirty-day comment period.[55] The modifications became final in August 2002.[56] Most health plans, health care providers and health care clearinghouses were required to be in compliance with HIPAA privacy regulations by April 2003.[57]

When the Bush administration proposed changes to the privacy regulations that would ease the consent requirements, some members of Congress expressed deep concern that these changes would erode an individual's privacy protections as afforded in the December 2000 final regulations.[58] Specific concern was raised that the administration was responding to the demands of the health care corporations, favoring corporate America over individuals.[59] Others viewed the changes as "an elegant balance between American privacy dogma and health care quality and technology,"[60] recognizing that "health information, used in the right hands and with the right safeguards, can lead to improved health and advances in research, [but] should not be used with disregard for patient privacy."[61]

The main difference between the two sets of "final" regulations is the relaxation of pre-disclosure consent requirements and the enhancement of the notice requirement as the tool for engaging patients in conversations regarding their expectations of privacy.[62] These changes are highly controversial,[63] as advocates of the change see it as necessary to remove the unintended detrimental effects on treatment that a prior consent requirement would have caused,[64] while opponents argue that removing the consent re-

54. *Id.* at 53,183, 53,193–94, 53,210–11.

55. *Id.* at 53,183.

56. *Id.* at 53,182.

57. *Id.* at 53,183.

58. *See* 148 CONG. REC. S2311-08 (2002) (remarks of Senators Kennedy and Dodd).

59. *Id.*

60. Jennifer M. Smith, *Balancing Privacy and Commerce: New Medical Accountability Rules Elegantly Blend Needs of Patients and Medical Providers*, PALM BEACH DAILY BUS. REV., Sept. 23, 2002, at 13.

61. HPP BEST PRINCIPLES, *supra* note 2, at 7.

62. Privacy Rule, 67 Fed. Reg. at 53,210–11.

63. *See* Jennifer Ascher et al., *HIPAA Standards for Privacy of Individually Identifiable Health Information: An Introduction to the Consent Debate*, 35 J. HEALTH L. 387, 390–91 (2002).

64. *See, e.g.*, Kristen Rosati, *DHHS Wisely Proposed to Remove the "Consent" Requirement from the HIPAA Privacy Standards*, 35 J. HEALTH L. 395 (2002).

quirement erodes the privacy protections intended by HIPAA in service of the needs of the vocal health care industry.[65]

2. Purpose

Standards to protect the privacy of health information were considered necessary to protect the confidentiality of health information which would be increasingly challenged by the

> complexity of the health care industry, and by advances in the health information systems technology and communications . . . . In an era where consumers are increasingly concerned about the privacy of their personal information, the Privacy Rule creates, for the first time, a floor of national protections for the privacy of their most sensitive information—health information. Congress has passed other laws to protect consumers' personal information contained in bank, credit card, other financial records, and even video rentals. These health privacy protections are intended to provide consumers with similar assurances that their health information, including genetic information, will be properly protected.[66]

The December 2000 Privacy Regulations were guided by five principles: 1) consumer control—consumers should not have to trade their health privacy in order to obtain health care; 2) boundaries—disclosure of health information should be for health care reasons only; 3) security—consumers should have faith that their health information will be protected; 4) accountability—punishment for misuse of information; and 5) public responsibility—privacy should be balanced with the need to support medical research and law enforcement.[67] Presumably the same principles guided the August 2002 Privacy Regulations, although none were clearly articulated.

3. Main Provisions

Under the Privacy Rule, health care providers, health plans, and health care clearinghouses "must guard against misuse of individuals' identifiable health information and limit the sharing of such information, and [health care] consumers are afforded significant new rights to enable them to understand and control how

65. *See, e.g.*, Geralyn A. Kidera, *The Proposed Changes to the Final Privacy Rule Suggest a Disturbing Reduction in an Individual's Ability to Exercise a Right to Healthcare Privacy*, 35 J. HEALTH L. 403 (2002).

66. Privacy Rule, 67 Fed. Reg. at 53,182.

67. Press Briefing by Donna Shalala, Secretary of Health and Human Services, The White House, 2000 WL 1868717 (Dec. 20, 2000).

their health information is used and disclosed."[68] The regulation creates a blanket prohibition for all "covered entities"—defined as health plans, health care clearinghouses, and health care providers that engage in certain electronic transactions[69]—prohibiting their use or disclosure of protected health information (PHI).[70] PHI is defined as individually identifiable health information—information that is created or received by a covered entity relating to the past, present, or future condition, provision of health care or payment that identifies an individual or from which an individual may be identified—that is transmitted or maintained by electronic media, or in any other form or medium.[71] Excluded from the definition of PHI are certain records held by an employer for employment purposes or records covered under the Family Educational Rights and Privacy Act, which protects certain educational records of adult students at postsecondary institutions.[72]

Because of the blanket prohibition, any use or disclosure of PHI must meet an exception in order to not violate the Privacy Rule. A covered entity is permitted to use or disclose PHI: 1) to the individual; or 2) for treatment, payment, or health care operations purposes; or 3) pursuant to a HIPAA compliant authorization; or 4) as otherwise required.[73] A covered entity must disclose PHI when the individual so requests.[74] A covered entity must also disclose PHI when required to do so by HHS as part of a compliance investigation.[75] When disclosing, other than for treatment or to the individual or HHS, the covered entity should disclose only that which is minimally necessary to accomplish the intended purpose of the disclosure.[76] A covered entity seeking to engage in marketing activities or to use or disclose psychotherapy notes must obtain an authorization.[77] If a covered entity seeks to use or disclose PHI in

68. Privacy Rule, 67 Fed. Reg. at 53,182.

69. 45 C.F.R. § 160.102 (2003).

70. § 164.502.

71. § 160.103.

72. *Id.* For more information regarding the interaction of HIPAA and Family Educational Rights and Privacy Act, see Pietrina Scaraglino, *Complying with HIPAA: A Guide for the University and Its Counsel*, 29 J.C. & U.L. 525, 537 (2003).

73. 45 C.F.R. § 164.502(a).

74. § 164.502(a)(2); *see also id.* §§ 164.524, 164.528. Prior to the Privacy Rule, there was no federal law guaranteeing patient access to information, despite the fact that patients sometimes found it difficult to acquire or amend their records. *See* Privacy Rule, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000).

75. 45 C.F.R. § 164.502(a)(2).

76. § 164.502(b).

77. § 164.508. See *infra* text accompanying notes 119-125 for a discussion of authorization requirements.

the making of a facility directory, in involving others in the individual's care, or for notification purposes, the covered entity must inform the individual in advance and give her an opportunity to orally agree to, prohibit, or object to the use or disclosure of PHI.[78] No authorization is required for uses and disclosures required by law, as part of public health activities, for judicial or administrative proceedings, for health oversight activities, for information regarding a victim of abuse, for law enforcement purposes, for certain information about decedents, for certain information for donation and research purposes, to avert a serious threat to health or safety, for specialized government functions, or for workers' compensation.[79] Specific requirements for institutional fundraising are also enumerated, including, among other things, the requirement that an individual have a right to opt out of receiving any fundraising communications.[80]

Other protections are also provided. Prior to disclosing, a covered entity must: verify the identity of the person requesting the PHI and its authority to do so;[81] identify those employees who need access to PHI to carry out their duties and limit access to only those so identified; and implement policies and procedures to limit disclosures to the minimum necessary to accomplish the purpose of the disclosure.[82] The regulations also permit a covered entity to use information which is stripped of all identifying characteristics.[83]

The Privacy Rule creates rights for individuals to access their health information. Upon request, covered entities must permit an individual to inspect and obtain a copy of her PHI,[84] request amendment to her PHI,[85] and receive an accounting of all of the uses and disclosures of the PHI made by the covered entity.[86] Individuals may also request that the covered entity restrict the use and disclosure of PHI and communicate with them confidentially.[87]

78. 45 C.F.R. § 164.510. The entity may inform the patient orally and may receive agreement or objection orally. This is a substantially lower burden than securing a HIPAA compliant authorization. See *infra* text accompanying notes 119–125.

79. 45 C.F.R. § 164.512.

80. § 164.514(f).

81. § 164.514(h).

82. § 164.514(d).

83. § 164.514(a). Such information is called "de-identified" information under the Privacy Rule. *Id.*

84. § 164.524.

85. § 164.526.

86. § 164.528.

87. § 164.522.

Finally, the Privacy Rule requires that covered entities: designate a privacy officer to oversee all privacy activities and receive complaints; train its workforce concerning proper privacy protections; create reasonable safeguards to protect the privacy of health information; create a complaint process; document privacy policies and procedures; impose sanctions against employees who violate privacy policies; refrain from intimidating or hostile acts against complainants; and mitigate any harmful effect due to the use or disclosure of PHI.[88] The covered entity cannot require individuals to waive their rights under the Privacy Rule in order to receive treatment, payment, enrollment, or eligibility for benefits.[89]

HHS's Office for Civil Rights (OCR) is in charge of administering, and ensuring compliance with, the Privacy Rule.[90] Compliance will generally be complaint-driven, although OCR has the authority to initiate investigations on its own.[91] OCR has created a Fact Sheet detailing how an individual may file a complaint.[92] At the outset, OCR is relying upon voluntary compliance and is anticipating that education will resolve most issues.[93] Penalties for violating the Privacy Rule include civil monetary fines imposed on a covered entity.[94] Criminal penalties are available for knowing, willful violations, or violations with the intent to sell or use PHI for personal gain or malicious harm.[95]

4. Notice of Privacy Practices

In place of a pre-use or disclosure consent, the 2002 modification to the Privacy Rule imposed a stronger notice requirement.[96] Covered entities are required to provide "adequate notice of the uses and disclosures of protected health information that may be

88. § 164.530.

89. § 164.530(h).

90. Office for Civil Rights; Statement of Delegation of Authority, 65 Fed. Reg. 82,381 (Dec. 28, 2000).

91. 45 C.F.R. §§ 160.306, 160.308. *See* Joyce Frieden, *HIPAA Privacy Rule: It's Not Too Late to Comply*, FAM. PRAC. NEWS, Mar. 15, 2003, at 1 ("Any enforcement of the penalties will be driven by complaints filed against providers.").

92. OFFICE FOR CIVIL RIGHTS, DEP'T OF HEALTH & HUMAN SERVS., FACT SHEET: HOW TO FILE A HEALTH INFORMATION PRIVACY COMPLAINT WITH THE OFFICE FOR CIVIL RIGHTS, *available at* http://www.os.hhs.gov/ocr/privacyhowtofile.htm (last visited Dec. 6, 2004).

93. *HIPAA Privacy Guidance Seeks to Maximize Voluntary Enforcement; Enforcement Rule is in Drafting Stage*, HOSP. ACCESS MGMT., Feb. 2003, at S1.

94. HIPAA, Pub. L. No. 104-191, § 1176, 110 Stat. 1936, 2028 (1997) (codified at 42 U.S.C. § 1320d-5 (2000)).

95. § 1177, 110 Stat. at 2029 (codified at 42 U.S.C. § 1320d-6 (2000)).

96. Privacy Rule, 67 Fed. Reg. 53,182, 53,210–11 (Aug. 14, 2002).

made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information."[97]

The notice is intended to focus individuals on privacy issues and concerns, to prompt them to have discussions with their health plans and health care providers, and to encourage them to exercise their rights.[98] Commentators have made clear, however, that the notice requirements do not demand that the patient understand what is being disclosed.[99]

The information being given to providers regarding their responsibilities with respect to patient understanding is rather troubling. Although it is unreasonable to expect that every ill, possibly uneducated healthcare consumer could achieve actual understanding, the fact that HHS has linked enforcement to individual complaints indicates that those members of society who are unable to understand the NPP may be unable to enforce their rights, and thus may not receive the full protection of the law. On the other hand, "even if few individuals avail themselves of the opportunity to learn the details of an organization's policies and practices, their ability to do so can serve a useful purpose,"[100] such as allaying fears

97. 45 C.F.R. § 164.520(a)(1).

98. Privacy Rule, 67 Fed. Reg. at 53,238–41; OFFICE FOR CIVIL RIGHTS, DEP'T OF HEALTH & HUMAN SERVS., STANDARDS FOR THE PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION GUIDANCE (Revised April 3, 2004), at 40, *available at* http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf [hereinafter HHS GUIDANCE].

99. *Notice of Privacy Practices: Your First Patient Contact the Morning of April 14*, REP. PATIENT PRIVACY, Oct. 2002, at 1 ("It's important to remember that covered entities are required to provide privacy notices and, whenever possible, get acknowledgment of a patient's receipt of the notice. Covered entities are *not required to make sure the notices are read or understood* by patients.") (emphasis added); *see also* Privacy Rule, 67 Fed. Reg. at 53,241. Many commentators have identified the understanding expectation as a factor that differentiates the HIPAA NPP from the informed consent process. *E.g.*, *Consider These Factors When Deciding on Your Policies on Consent*, 2 REP. PATIENT PRIVACY, Oct. 2002 at 1("[I]t's another ball of wax from the informed consent concept . . . ."); Jeffrey A. Lovitky, *The Privacy of Health Information: Consents and Authorizations under HIPAA*, FLA. B.J., May 2002, at 10 ("It must be emphasized that the HIPAA consent is conceptually different from . . . informed consent . . . ."). Although the comparison may be helpful to promote understanding of the NPP requirement within the health care industry itself, it is somewhat misleading, because the legal requirements of informed consent do not demand patient understanding. The legal focus is on a physician's proper disclosure, not a patient's comprehension. *See* Canterbury v. Spence, 464 F.2d 772, 780 n.15 (D.C. Cir. 1972).

100. Matthew K. Wynia et al., *Shared Expectations for Protection of Identifiable Health Care Information*, 16 J. GEN'L INTERNAL MED. 100, 104 (2001).

of misuse of health information that often lead individuals to avoid testing or treatment. Moreover, forcing sunlight on the policies may encourage "information trustees [to] carefully consider what those policies should be."[101]

The notice is required to be in "plain language"[102] and must include the following statements:

1) A header that reads: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."[103]
2) The uses and disclosures, including a description and at least one example, that a covered entity may make with respect to treatment, payment, and health care operations, a description of each of the other purposes for which the covered entity is permitted or required to use or disclose PHI without authorization, and a statement that other uses or disclosures will be made only with the patient's written authorization, which the patient may revoke at any time.[104] The descriptions must "include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required" by law.[105]
3) If the covered entity intends to contact the individual to provide appointment reminders, treatment alternatives, or other health benefits or services, to fundraise, or if a group health plan intends to disclose PHI to the plan sponsor, then the NPP must state this specifically.[106]
4) The individual's rights, including the right to restrict use or disclosure of PHI, receive confidential communications, inspect or copy PHI, amend PHI, receive an accounting of disclosures, and if receiving the notice electronically, the right to receive a paper copy.[107]
5) The covered entity's duties, including the duty to "maintain the privacy of [PHI] and to provide individuals with notice of its legal duties and privacy practices with respect to

101. *Id.* at 103–04.
102. 45 C.F.R. § 164.520(b)(1).
103. § 164.520(b)(1)(i).
104. § 164.520(b)(1)(ii)(A)–(E).
105. § 164.520(b)(1)(ii)(D).
106. § 164.520(b)(1)(iii).
107. § 164.520(b)(1)(iv).

[PHI]."[108] It must also contain a statement that the entity is required to abide by the terms of the notice, and that it reserves the right to change the terms of its notice making the new notice effective for all PHI, including a description of how it will provide individuals with revised notice.[109] A new notice must be distributed in a timely fashion when a covered entity makes any material changes to its privacy practices.[110]

6) That an individual may lodge a complaint with HHS or with the covered entity, including a brief description of how the individual may complain to the entity and a statement that she will not be retaliated against for complaining.[111]
7) A contact name or title and telephone number of a person within the covered entity that individuals may contact for more information.[112]
8) An effective date of the notice.[113]

If the covered entity has chosen to limit its uses or disclosures of PHI, it may describe such limited uses in its notice, as long as it does not limit those uses or disclosures that it is required to make.[114] If the covered entity wants any changes it makes to its privacy practices to apply to PHI collected prior to notification of the changes, then it must include the language above regarding reserving the right to modify its practices.[115]

Health plans must make the NPP available to individuals covered by the plan, and health care providers must post the notice in a clear and prominent location where it is reasonable to expect that the patient will see it, and make copies available to those who wish to take it with them.[116] Health care providers must provide the notice by the date of first service delivery after compliance date, and must make a good faith effort to obtain written acknowledgement of receipt of the notice.[117] Those covered entities that are required to provide a notice may not use or disclose PHI "in a manner inconsistent with such notice."[118]

108. § 164.520(b)(1)(v)(A).
109. § 164.520(b)(1)(v)(B)–(C).
110. § 164.520(b)(3).
111. § 164.520(b)(1)(vi).
112. § 164.520(b)(1)(vii).
113. § 164.520(b)(1)(viii).
114. § 164.520(b)(2)(i).
115. § 164.520(b)(2)(ii).
116. § 164.520(c).
117. § 164.520(c)(2).
118. § 164.502(i).

5. Authorizations

Should a covered entity seek to use or disclose PHI for marketing purposes, or use or disclose psychotherapy notes (other than use by the creator of the notes to carry out treatment, or use by the entity for training or to defend itself in a legal action), or any other use or disclosure not otherwise permitted by the Privacy Rule, it must obtain a valid authorization.[119] A valid authorization must be written in plain language,[120] a copy must be provided to the individual,[121] and it must include at least the following elements:

1) a specific and meaningful description of the information to be used or disclosed;
2) the name or other specific identification of the person or class of persons authorized to make the requested use or disclosure;
3) the name or other specific identification of the person or class of persons to whom the PHI will be used or disclosed;
4) a description of the purpose of the requested use or disclosure;
5) an expiration date or expiration event;
6) the signature of the individual and the date;[122]
7) statements that indicate the individual's right to revoke the authorization in writing[123] and the exceptions to the right to revoke, the potential that information disclosed could be "subject to redisclosure by the recipient and no longer be protected" by the Privacy Rule,[124] and the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization.[125]

D. Critique of the Privacy Regulations

Much has been written about HIPAA and the Privacy Rule. It has been described as "a maze of mandates and exceptions,"[126]

119. § 164.508(a).
120. § 164.508(c)(3).
121. § 164.508(c)(4).
122. § 164.508(c)(1).
123. § 164.508(c)(2)(i).
124. § 164.508(c)(2)(iii).
125. § 164.508(c)(2)(ii). Generally, treatment, payment, enrollment and eligibility may not be conditioned on authorization, but research-related treatment may be conditioned, as well as other very limited activities of health plans and PHI involving a third party. *See* § 164.508(b)(4).
126. Nancy A. Lawson et al., *The HIPAA Privacy Rule: An Overview of Compliance Initiatives and Requirements*, 70 DEF. COUNS. J. 127, 127 (2003).

"enormously broad,"[127] "likely to produce the most significant change in health care operations since Medicare,"[128] the "most sweeping piece of legislation to affect the health care industry in decades,"[129] and a "remarkably effective and flexible 'first cut' at making medical information privacy a reality."[130] As this section will explore, major critiques of the rule argue that the rule is confusing, difficult to implement, a failure in achieving actual information privacy, or illegal either because it is beyond the scope of authority of HHS or unconstitutional.

Due to the complicated history of the privacy rule, there seems to be some confusion as to what is exactly required. For example, in January 2003, *Healthcare Risk Management* published an article stating that providers must obtain consent before using or disclosing PHI for treatment, payment or health care operations and that providers may condition treatment upon such consent.[131] This is not true under the modified Privacy Rule published in 2002, in which the consent requirement was made optional.[132] As another example, *The New York Times* reported that a doctor calling a hospital could not obtain information concerning his own patient because the emergency room doctor would not discuss the patient's care for fear of violating the rules.[133] This is an unduly cautious interpretation of the Privacy Rule, because disclosures necessary for treatment purposes, including consultation between health care providers, are permitted.[134]

127. Mary Beth Johnston & Leighton Roper, *HIPAA Becomes Reality: Compliance with New Privacy, Security, and Electronic Transmission Standards*, 103 W. VA. L. REV. 541, 542 (2001).

128. Kathryn L. Bakich, *Countdown to HIPAA Compliance: Understanding EDI, Privacy, and Security*, BENEFITS L.J., Summer 2002, at 45.

129. Michael N. Mercurio, *Uncomplicating Health Care Industry Via HIPAA's Administrative Simplification*, MD. B.J., Feb. 2003, at 36.

130. Jack Rovner, *Some Advice on Consent: Legislators and Providers Need to Look Closer at the Reality of Medical Privacy*, MOD. HEALTHCARE, May 6, 2002, at 21.

131. *HIPAA Regulatory Alert: How to Draft Documents for HIPAA Implementation: Know Requirements for Consent, Covered Entities*, HEALTHCARE RISK MGMT., Jan. 1, 2003, at SSS7.

132. Frederick Ryland, *Federal Health Privacy Comes to Maryland: What's the Big Deal?*, MD. B.J., Feb. 2003, at 27, 29.

133. Robert Pear, *Health System Warily Prepares for New Privacy Rules*, N.Y. TIMES, Apr. 6, 2003, at A26 (quoting the inquiring physician: "'I don't know who was right legally, but I do know that the rules are creating a lot of confusion.'").

134. 45 C.F.R. §§ 164.501, 164.506; *see* HHS GUIDANCE, *supra* note 98, at 20–24.

Some of the confusion stems from vague language in some of the key provisions of the Privacy Rule.[135] For example, covered entities may disclose only the minimum necessary to satisfy the purpose of the disclosure.[136] Anticipating what the minimum necessary disclosure would be can be extremely difficult, "creat[ing] significant burdens in even the most routine, daily processes, perhaps even leading to reduced quality in patient care."[137] What may be unnecessary from one person's perspective may be critical for others in the delivery of proper patient care; "[i]t is impossible to determine in advance what information may be necessary for another caregiver that may be seeing the patient for another reason."[138] Other terms such as "reasonable efforts"[139] and "incidental use or disclosure"[140] can also be ambiguous.[141]

Concern about implementing the rule has spawned numerous articles presenting an overview of the requirements and steps to implementation.[142] HHS estimates that implementation of the privacy rule will cost in excess of 3.8 billion dollars over five years, while some members of industry estimate that it will cost ten times that amount.[143]

---

135. *See* Brian Zoeller, *Health and Human Services' Privacy Proposal: A Failed Attempt at Health Information Privacy Protection*, 40 BRANDEIS L.J. 1065, 1077–78 (2002).

136. 45 C.F.R. § 164.502(b).

137. Zoeller, *supra* note 135, at 1078.

138. Rick Pollack, American Hospital Ass'n, Detailed Comments, *Standards for Privacy of Individually Identifiable Health Information*, 13 (Feb. 17, 2000), *available at* http://aspe.os.dhhs.gov/admnsimp/nprm/comments/231537.pdf.

139. 45 C.F.R. § 164.502(b) (requiring covered entities to "make reasonable efforts to limit" PHI disclosure).

140. *Id.* § 164.502(a)(1) (permitting covered entities to disclose protected health information "incident to a use or disclosure otherwise permitted").

141. 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, 164–66 (2003).

142. *See, e.g.*, Bakich, *supra* note 128, at 45; Hugh Barton, *Health Information and Patient Rights under HIPAA*, 65 TEX. B.J. 824 (2002); Susan M. Gordon, *Privacy Standards for Health Information: The Misnomer of Administrative Simplification*, 5 DEL. L. REV. 23 (2002); Johnston & Roper, *supra* note 127; Lawson et al., *supra* note 126.

143. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 60,006–07 (Nov. 3, 1999) (to be codified at 45 C.F.R. pts. 160, 164) (Proposed Rule); Colletti & Pachman, *supra* note 39, at 16; *Confidentiality of Patient Records: Hearing before the Subcomm. on Health of the House Comm. on Ways and Means*, 106th Cong., 53–54 (2000) (statement of Alissa Fox, Executive Director, Office of Policy and Representation, Blue Cross and Blue Shield Association); Trinita C. Robinson, *HIPAA's Privacy Standards Require Understanding and Action*, 55 HEALTHCARE FIN. MGMT. 66, 69 (2001).

Part of the challenge of implementation depends upon whether HIPAA applies or whether state law pre-empts the Privacy Rule. Generally, HIPAA pre-empts state law, but whenever state law provides more stringent protections than are provided under the Privacy Rule, state law controls.[144] Confusion over this issue has caused at least one commentator to argue for a broad-based federal law that pre-empts all state law in this area.[145]

Beyond the implementation challenges, debate exists as to whether the Privacy Rule actually achieves its goals. Some commentators argue that instead of protecting patient privacy, the Privacy Rule actually permits disclosures of a patient's sensitive information without true notice or consent and without a legitimate justification.[146]

Others argue that the regulations go beyond HHS' scope of authority because they apply not only to entities that engage in electronic transactions, but require those entities to ensure that their business partners, such as medical transcription services and answering services, also comply.[147] Still others argue that the regulations do not go far enough because they permit disclosures for direct marketing.[148]

While the HIPAA regulations may be inadequate to truly protect the privacy of health information, they are a starting point. Even though the rules do not create a federal private right of action for individuals who are injured, they may be helpful in state common law breach of confidentiality claims.[149] For instance, they may

144. 45 C.F.R. § 160.203(b); *see* Neville M. Bilimoria, *Contending with HIPAA Privacy Standards in Illinois*, 90 ILL. B.J. 414 (2002); Jane F. Clemens, *New Federal Regulations Expand Protections for Privacy of Health Records*, N.Y. ST. B.J., June 2002, at 37; Guthrie, *supra* note 141, at 149–50; Ryland, *supra* note 132, at 28–29; Zoeller, *supra* note 135, at 1078–80.

145. Rebecca H. Bishop, Note, *The Final Patient Privacy Regulations under the Health Insurance Portability and Accountability Act—Promoting Patient Privacy or Public Confusion?*, 37 GA. L. REV. 723 (2003).

146. Mike Hatch, *HIPAA: Commercial Interests Win Round Two*, 86 MINN. L. REV. 1481, 1494 (2002). Hatch rejects the argument that communal interests in medical information necessitate disclosure by pointing out that no justification has been offered as to why an individual's identifying information must be attached to the health data to fulfill the legitimate communal interests in research and government oversight. *Id.* at 1492–93.

147. Zoeller, *supra* note 135, at 1074–76.

148. James D. Molenaar, *The HIPAA Privacy Rule: It Helps Direct Marketers Who Help Themselves to Your Personal Health Information*, 2002 L. REV. M.S.U.-D.C.L. 855, 884 (2002).

149. "The vast majority of states recognize that an actionable tort lies for a physician's breach of the duty to maintain the confidences of his or her patient in

be used as evidence of a standard of care below which the provider may not fall.[150] Further, HIPAA's business associate agreements requirement might create a sufficient responsibility to hold liable those entities not in direct privity with the patient, and therefore not in a position of trust as required by the confidentiality tort.[151]

HIPAA and the Privacy Rule have survived at least three legal challenges to date. In 2003, the Fourth Circuit found that Congress did not impermissibly delegate its legislative role because it included an intelligible principle which HHS could follow in promulgating regulations, HHS did not exceed the scope of its authority by including non-electronic records in the Privacy Rule, and neither HIPAA nor the Privacy Rule were impermissibly vague.[152] In addition, the Privacy Rule has withstood a Fourth Amendment challenge that giving the government unrestricted access to medical records is an unreasonable search or seizure, a First Amendment challenge that giving unrestricted access will chill speech between patients and physicians, and a Tenth Amendment challenge that it goes beyond Congress' Commerce Clause power to regulate an issue generally left to the states.[153] Most recently, a federal district court in Pennsylvania ruled that the 2002 Privacy Rule amendment making consents for disclosure optional did not violate First Amendment free speech rights or the Fourth and Ninth Amendment privacy and property rights, and further, that the process by which the amendment was promulgated did not violate the Administrative Procedure Act.[154]

---

the absence of a compelling public interest . . . ." Winn, *supra* note 3, at 654. Winn argues that the right to privacy will not be helpful in the case of limited inadvertent disclosures of health information because publication and intent elements will not be satisfied. Therefore, he suggests that a breach of confidentiality tort will be more effective in vindicating patients' rights. *See id.* at 652–61.

150. *See* Ronald J. Levine & Anne Maltz, *HIPAA Regulations' Unintended Effect: Civil Actions for Inappropriate Disclosure of Patient's Medical Information May Increase*, N.Y. L.J., July 2, 2001, at 7 (suggesting that HIPAA can be used as the standard by which medical professionals' behavior is judged in certain tort actions).

151. Winn, *supra* note 3, at 672–74.

152. South Carolina Med. Ass'n v. Thompson, 327 F.3d 346 (4th Cir. 2003), *cert. denied*, 124 S. Ct. 464 (2003).

153. Ass'n of Am. Physicians & Surgeons, Inc. v. U.S. Dep't of Health & Human Servs., 224 F. Supp. 2d 1115 (S.D. Tex. 2002), *aff'd*, No. 02-20792, 2003 WL 21196194 (5th Cir. May 15, 2003). Plaintiffs also claimed that the Privacy Rule violated the Regulatory Flexibility Act and the Paperwork Reduction Act by failing to consider the effect on small health plans and health care providers. Both of these claims were dismissed as well. *Id.* at 1128–29.

154. Citizens for Health v. Thompson, 2004 U.S. Dist. LEXIS 5745 (E.D. Pa. Apr. 2, 2004).

This article focuses on whether the Privacy Rule as constructed is internally inconsistent because it relies on disclosure to individuals as the primary means of engaging health care consumers in control over their health information, yet makes little or no attempt to ensure that consumers understand the disclosure. Against the background presented above, the next section examines the Notice of Privacy Practices.

II.
THE PLAIN LANGUAGE REQUIREMENT

The Privacy Rule requires that the NPP be "written in plain language."[155] Other than limited discussion in the preamble[156] and a guide on plain language made available after the date by which covered entities were required to comply,[157] the regulation itself does not address what constitutes plain language. As explained in the next part, the mere requirement that the NPP be written in plain language does not ensure that the NPP is sufficiently comprehensible to the general public to instill confidence that the NPP adequately involves individuals in the privacy of their health information. Because enforcement of the Privacy Rule rests on individual complaints,[158] it is important that the individual understands his or her rights and the requirements of the law. It is also important that there be some standard for evaluating whether an NPP has been written in plain language. Although the Privacy Rule fails to specify an evaluation method, some guidance may be found in the preamble and the plain language literature.

A. The Background of Plain Language in Legal Writing

For nearly three decades, advocates of simplifying legal writing have argued for the use of plain language in the construction of legal documents.[159] As Rudolf Flesch, a noted theorist on plain language writing, observed, "[m]ost people don't read legal papers, [and] labels . . . . When they do read . . . such things, they usually

155. 45 C.F.R. § 164.520(b)(1). While this discussion will focus on the Notice of Privacy Practices, much of the same analysis could be applied to the limited authorizations required by the Rule. *See supra* Part I.C.5.

156. *See infra* text accompanying note 182.

157. *See infra* text accompanying note 172.

158. *See supra* text accompanying notes 90–92.

159. *E.g.*, RUDOLF FLESCH, HOW TO WRITE PLAIN ENGLISH: A BOOK FOR LAWYERS AND CONSUMERS (1979); RONALD L. GOLDFARB & JAMES C. RAYMOND, CLEAR UNDERSTANDINGS: A GUIDE TO LEGAL WRITING (1982); *see* DAVID MELLINKOFF, THE LANGUAGE OF THE LAW 422–23 (1963).

don't understand them. If you're writing for 'the general public,' you'd better remember this basic fact of life."[160] To promote greater public understanding advocates argue that plain language should be a general rule for legal documents.[161] Certainly, greater understanding is the impetus behind the plain language requirement in the Privacy Rule.[162]

It has been shown that legal concepts can effectively be communicated in plain language.[163] For example, a classic study of consumer contract comprehension found that "simplifying [the] drafting style increases comprehension."[164] In addition to increased comprehension, judges and clients prefer plain language.[165] Moreover, using plain language can save money by enhancing efficiency and reducing confusion.[166]

Many federal and state laws have required that certain documents be written simply and understandably.[167] One of the more

160. FLESCH, *supra* note 159, at 8.

161. *Id.*

162. Privacy Rule, 65 Fed. Reg. 82,462, 82,723 (Dec. 28, 2000) ("We require . . . plain language so that the average reader will be able to understand the notice.").

163. Peter Butt, *The Assumptions Behind Plain Legal Language*, 32 H.K. L.J. 173, 177–83 (2002).

164. Michael E.J. Masson & Mary Anne Waldron, *Comprehension of Legal Contracts by Non-Experts: Effectiveness of Plain Language Redrafting*, 8 APPLIED COGNITIVE PSYCHOL. 67, 77 (1994). In addition, several studies on jury instructions indicate that jurors have an alarmingly low level of comprehension of their instructions and suggest that simplified language could improve understanding. For general discussion of the jury instruction problem, see John P. Cronan, *Is Any of this Making Sense? Reflecting on Guilty Pleas to Aid Criminal Juror Comprehension*, 39 AM. CRIM. L. REV. 1187 (2002); Dylan Lager Murray, *Plain English or Plain Confusing?*, 62 MO. L. REV. 345 (1997); Judge Roger M. Young, *Using Social Science to Assess the Need for Jury Reform in South Carolina*, 52 S.C. L. REV. 135 (2000).

165. Butt, *supra* note 163, at 184–85 (referencing studies showing that 80% of judges prefer pleadings written in plain language, and that lay persons prefer plain language documents).

166. *Id.* at 183 ("[B]y rewriting documents into plain language, enquiries from customers about meaning are reduced which allows the company to redeploy enquiry staff to other tasks.").

167. *E.g.*, Employee Retirement Security Act of 1974, 29 U.S.C. § 1022(a)(1) (2000) (requiring that plan participants be given a plan description written to be "understood by the average plan participant"); Magnuson-Moss Warranty-Federal Trade Commission Improvement Act, 15 U.S.C. § 2302 (2000) (requiring warranties to be written in "simple and readily understand[able] language"); President Carter's 1978 executive order declaring that all federal regulations "shall be as simple and clear as possible." Exec. Order No. 12,044, 43 Fed. Reg. 12,661 (March 23, 1978), *revoked by* Exec. Order No. 12,291, 46 Fed. Reg. 13,913 (Feb. 17, 1981). Many states have considered or enacted plain language legislation in the area of consumer contracts. For a brief overview of the history of plain language initia-

notable plain language requirements appears in the federal securities regulations. After piloting a program that required selected companies to draft prospectuses and other securities documents in plain language designed to be "clear, well-written and . . . [to] increase investors' understanding," the Securities and Exchange Commission (SEC) adopted plain language rules for all prospectuses.[168] The rule requires drafting portions of the prospectus in compliance with six plain language principles: "Short sentences; Definite, concrete, everyday words; Active voice; Tabular presentation or bullet lists for complex material, whenever possible; No legal jargon or highly technical business terms; and No multiple negatives."[169] The SEC prepared a handbook to help guide the production of investor materials in accordance with its plain language requirements, in which it emphasizes the importance of knowing your audience, knowing what information must be disclosed, and using clear writing.[170]

Like the NPP, SEC investor materials are part of a disclosure-based regulatory scheme. The analogy between securities documents and health information privacy practices is not perfect because investors do not represent as broad a public as consumers of health care. Still, it can be instructive. Despite a narrower, presumably more sophisticated target audience, the SEC specifies the type of writing and format and even has a handbook to "enable issuers to improve dramatically the clarity of their disclosure documents."[171] If it is important for the SEC to specify plain language expectations, it seems even more important for HHS, where the disclosure is going to a broader-based public. Although HHS has made a guide to plain language available on their website,[172] the

tives, see Michael S. Friman, *Plain English Statutes: Long Overdue or Overdone?*, 7 LOY. CONSUMER L. REP. 103, 104–06 (1995); FLESCH, *supra* note 159, at 1–2.

168. Securities & Exchange Commission, Plain English Disclosure, 63 Fed. Reg. 6,370, 6,371 (Feb. 6, 1998) [hereinafter SEC, Plain English].

169. 17 C.F.R. § 230.421(d) (2003).

170. SEC. & EXCH. COMM'N, OFFICE OF INVESTOR EDUC. & ASSISTANCE, A PLAIN ENGLISH HANDBOOK: HOW TO CREATE CLEAR SEC DISCLOSURE DOCUMENTS (1998). For a general discussion of SEC plain language disclosure, see Kenneth B. Firtel, Note, *Plain English: A Reappraisal of the Intended Audience of Disclosure under the Securities Act of 1933*, 72 S. CAL. L. REV. 851 (1999).

171. SEC, Plain English, 63 Fed. Reg. at 6,371. "We have seen marked improvement in the clarity of the disclosure when pilot participants have used these widely recognized basic principles of clear writing." *Id.*

172. Dept. of Health & Human Serv., Health Res. & Serv. Admin., Plain Language Principles & Thesaurus for Making HIPAA Privacy Notices More Readable, *available at* ftp://ftp.hrsa.gov/hrsa/hipaaplainlang.pdf (last visited November 22, 2004).

guide did not become available until after April 2003, the date by which healthcare providers were required to comply with the Privacy Rule and make their NPPs available to patients. Moreover, the guide is not posted conspicuously on the website, and it is unclear whether and to what extent covered entities are aware of it. This guide would have been a useful tool had it been available earlier, but in light of the complexity of amending an NPP[173], the guide's usefulness to covered entities after the broad scale April 2003 implementation is questionable.

Plain language is certainly not a panacea for all legal comprehension problems. It has often been critiqued for its inability to render documents more understandable, and for creating less legally accurate documents.[174] Critics argue that because of its highly conceptual nature, effective legal writing can neither be supplanted, nor made more understandable, just by requiring the "arbitrary" rules or "meaningless platitudes" of plain language.[175] One commentator argues that the use of plain language drafting should be limited to those documents for which ease of understanding is of primary importance.[176] The fact that plain language may actually obscure meaning does not apply to the NPP. Ease of understanding should be a primary purpose of the NPP, whose function is to disclose to the general public how health information will be used, disclosed, and protected. The legal concepts involved are less important than informing the public about how their PHI may be used or disclosed. HHS has indicated in numerous places that the NPP is supposed to spur conversations between individuals and providers regarding health information privacy.[177] For it to do this, individuals must understand the document. Although misunderstanding could also lead to conversation, "[o]ne of the goals of this rule is to create an environment of open communication and trans-

173. *See supra* notes 109, 110, 115.

174. Richard Hyland, *A Defense of Legal Writing*, 134 U. PA. L. REV. 599, 618–19 (1986) ("[L]egal concepts cannot be translated into Plain English by looking in a thesaurus . . . .").

175. *Id.* at 618 ("[I]t is either delusion or demagoguery to proclaim that those with no legal training might understand a legal document merely because their vocabulary includes all of the words in which it is written.").

176. He calls these persuasion documents, such as an appellate brief, whereby the author strives for understanding on a first read, as compared to preservation documents, such as wills, where expertise is often sought to interpret the meaning of the document. David Crump, *Against Plain English: The Case for a Functional Approach to Legal Document Preparation*, 33 RUTGERS L.J. 713 (2002).

177. *E.g.*, Privacy Rule, 65 Fed. Reg. 82,462, 82,549 (Dec. 28, 2000); Privacy Rule, 67 Fed. Reg. 53,182, 53,209, 53,238–41 (Aug. 14, 2002).

parency with respect to the use and disclosure of [PHI]. A lack of clarity in the notice could undermine this goal and create misunderstandings."[178]

Another critique of the plain language movement centers on the nature of the audience. The argument is that legislation is not drafted for the public, but rather for those working on its behalf, such as officers of the court, legislators, lawyers, and judges.[179] This critique also does not apply to the NPP—the audience of the NPP is clearly the general public. In fact, one commentator acknowledges that "[p]lain language has some value as far as making consumer contracts intelligible to the consumers . . . ,"[180] and would presumably agree that a notice intended for the public should be at least as intelligible as a consumer contract.

HHS' requirement that the NPP be written in plain language is appropriate, and none of the existing critiques of plain language counsel against it. However, HHS does not go far enough in defining plain language.

B. Privacy Rule Plain Language Requirement

The Privacy Rule simply states that the NPP must be "written in plain language."[181] Because the Privacy Rule does not spell out the specific requirements for making NPPs readable, we must look to the preamble and the literature on plain language to determine how to create a proper NPP and how to evaluate whether plain language has been achieved.

HHS provides some guidance in the rule preamble:

> A covered entity can satisfy the plain language requirement if it makes a reasonable effort to: organize the material to serve the needs of the reader; write short sentences in the active voice, using 'you' and other pronouns; use common, everyday words in sentences; and divide material into short sections. We do not require particular formatting specifications, such as easy-to-read design features (*e.g.*, lists, tables, graphics, contrasting colors, and white space), type face and font size. However, the purpose of the notice is to inform the recipients about their rights . . . . Recipients who cannot understand the [NPP] will miss important information . . . .[182]

178. Privacy Rule, 65 Fed. Reg. at 82,549.

179. Drury Stevenson, *To Whom Is the Law Addressed?*, 21 YALE L. & POL'Y REV. 105, 167 (2003).

180. *Id.* at 167.

181. 45 C.F.R. § 164.520(b)(1).

182. Privacy Rule, 65 Fed. Reg. at 82,548–49.

HHS' guidance is consistent with recommendations made by plain language experts. According to those experts, writers utilizing plain language techniques should eliminate excess words, write using the "'you' style" in which they address the reader directly and personally; eliminate definitions in legal documents by replacing them with straightforward explanatory phrases in the main text of the document; use examples whenever anything is complex and hard to explain; avoid double negatives (*e.g.*, "not unless" becomes "only if"; "it is unlawful to fail to" becomes "you must"); and minimize cross-referencing.[183] Moreover, advocates of clear writing suggest that a writer should think of her audience, not use jargon, and write concise, clear, simple words, sentences, and paragraphs.[184] Merely replacing "archaic terms and legalese" is not sufficient to greatly enhance comprehension.[185] "[R]educed . . . difficulty of vocabulary and shortened sentences" lead to the greatest improvements in comprehension, because "more familiar words . . . ma[ke] more concepts accessible to readers, and . . . shorter sentences [place] fewer demands . . . on working memory," making it easier for readers to form a "coherent, integrated representation of text."[186]

Once a document has been drafted, it must be evaluated to determine whether plain language has been achieved. There are two ways in which documents may be evaluated for their use of plain language: subjectively or objectively.[187] Some statutes, for example, employ an objective measurement by specifying the number of words permitted per sentence.[188] The most common method of objective measurement is the use of the Flesch Reading Ease Test.[189] Developed by Rudolph Flesch, the test determines readability by measuring the length of the words used and the number of words per sentence.[190] Each document is assigned a score from 0 to 100; the higher the score the more readable the document is;[191] the longer the words and sentences, the less readable the document

183. FLESCH, *supra* note 159, at 45, 68–69, 94–95.

184. GOLDFARB & RAYMOND, *supra* note 159, at 134–35, 146.

185. Masson & Waldron, *supra* note 164, at 78.

186. *Id.*

187. *See* Friman, *supra* note 167, at 106–07.

188. *See id.* at 107.

189. *See id.*

190. FLESCH, *supra* note 159.

191. For example, comic books generally receive a readability score of 90, while legislation receives a score of 40. Flesch argues that a score of 60 is plain language. *See* Friman, *supra* note 167, at 107.

is.[192] Although quite popular and in some cases quite effective, the Flesch test is unable to account for differences in grammar, ordering of words in a sentence, or the writer's use of words to convey complex concepts.[193]

Subjective evaluation occurs when the requirement that the document be written in plain language specifies only that, for example, the document be written in a "clear and coherent" manner.[194] While subjective measurement avoids some of the formulaic concerns that a strict adherence to an objective measurement presents, it has its own problems. Subjective measurements require that the evaluator place himself or herself in the position of the average reader. If this were easy, it seems unlikely that readability problems would arise in the first place. In other words, if highly educated drafters are subjectively evaluating the documents, and can do so effectively from the perspective of others less educated than themselves, how is it that there are still documents being written that are incomprehensible?

The Privacy Rule preamble guidance offers a subjective way of assessing plain language compliance. An entity is compliant by employing "short sections," "everyday words," and "short sentences."[195] Terms like "everyday" and "short" are open to interpretation and therefore subjective. Plus, the NPP should be written to "serve the needs of the reader,"[196] a classic subjective phrase. Finally, HHS seems to rely heavily on an assumption that entities will seek to provide the clearest possible notice to serve their own needs. "Covered entities have incentive to make their notice statements clear and concise. We believe the more understandable the notice is, the more confidence the public will have in the covered entity's commitment to protecting the privacy of health information."[197] While this may provide some incentive, other factors such as cost of pro-

192. *Id.*

193. David LaPrairie, Note, *Taking the "Plain Language" Movement Too Far: The Michigan Legislature's Unnecessary Application of the Plain Language Doctrine to Consumer Contracts*, 45 WAYNE L. REV. 1927, 1946–48 (2000). For example, "I went to the store."; "Went I to the store."; and "I goed to the store." receive the same Flesch score. *Id.* at 1947.

194. Friman, *supra* note 167, at 106.

195. Privacy Rule, 65 Fed. Reg. 82,462, 82,548 (Dec. 28, 2000).

196. *Id.*

197. Privacy Rule, 65 Fed. Reg. at 82,549. "Adequate notice can also help to build trust between patients and health care providers and organizations in so far as it removes the element of surprise about the use and disclosure of health information." Health Privacy Project, Comments on Final Federal Standards for Privacy of Individually Identifiable Health Information, at 9 (Mar. 2001), *available at* http://www.healthprivacy.org/usr_doc/55009.pdf.

duction (e.g., a longer notice or a multi-colored notice with graphics is more expensive), ease of administration, and general lack of competence to write a notice understandable from the patients' point of view may conflict with the entity's incentive to be clear.

While the regulations need not require a purely objective measure of readability, it is important for HHS to provide more guidance to help ensure the readability of the NPPs. The limited discussion in the preamble is inadequate because it is not an actual part of the regulations. Moreover, the preamble is, as one commentator put it, "longer than some versions of the Bible!"[198] People implementing the rule are unlikely to actually read it. The plain language guide is helpful, but because it was not available until after compliance was expected, and because it is unclear to what extent providers and other covered entities know of its existence, in practice, it provides little guidance. Since HHS relies on the NPP as central to the protection and reinforcement of health information privacy, the plain language requirement should be more explicit to remove some of the subjectivity and voluntary compliance notions implicit in the current Privacy Rule.

III.
THE NOTICE OF PRIVACY PRACTICES IS INSUFFICIENT

The previous section argued that the Privacy Rule's treatment of the NPP's plain language requirement is inadequate because it lacks the specificity needed to ensure the creation of a document in plain language. This section explores three other reasons why the privacy rule's reliance on the NPP does not achieve its goal of giving consumers control over their health information by educating them and involving them in the process of enforcing the proper uses and disclosures of their PHI. First, lessons learned from informed consent tell us that plain language in a document, while important, does not ensure understanding. Second, consumer information research tells us that too much information may impede understanding and the NPP information requirements are lengthy. Third, cognitive science tells us that people draw inferences from their experience and prior knowledge to help them interpret what they are reading. If patients have no prior knowledge of the range of ways in which their information may be used, and if the NPP focuses only on permissible uses, then patients have no experience

198. Mercurio, *supra* note 129, at 37.

or knowledge from which they may draw inferences regarding impermissible uses.

A. Plain Language Is Insufficient

Part II dealt with the inadequacy of how the plain language requirement is structured. This section uses an analogy to informed consent to argue that the NPP's plain language requirement is substantively insufficient to ensure that patients understand their rights with respect to health information privacy.

Informed consent is a process for obtaining "voluntary and knowledgeable . . . decision[s]" from patients regarding certain procedures, surgeries, and clinical research.[199] Informed consent includes "giving the participant understandable information . . . , providing ample opportunity . . . to consider all options and alternatives . . . , *ensuring that the participant comprehends the information* he or she is given, [and] obtaining . . . voluntary agreement . . . ."[200]

Despite institutional and legal requirements that informed consent documents be written in an understandable manner,[201] studies have shown that a significant number of informed consent forms are written at or near a college reading level.[202] Literacy ex-

199. Wendy K. Mariner & Patricia A. McArdle, *Consent Forms, Readability, and Comprehension: The Need for New Assessment Tools*, LAW, MED. & HEALTH CARE, Apr. 1985, at 68, 68.

200. Peter C. Raich et al., *Literacy, Comprehension, and Informed Consent in Clinical Research*, 19 CANCER INVESTIGATION 437, 439 (2001) (emphasis added). This quotation shows the sense within the health care industry that informed consent requires patient understanding. As discussed above, this may be a common perception within the industry, but it is not the current state of the law. *See supra* note 99.

201. *See* 21 C.F.R. § 50.20 (2003) (requiring informed consent for use of human subjects in FDA research be obtained using understandable language); 45 C.F.R. § 46.116 (2003) (requiring informed consent for use of human subjects in HHS research be obtained using understandable language); *see also* Lars Noah, *Informed Consent and the Elusive Dichotomy Between Standard and Experimental Therapy*, 28 AM. J.L. & MED. 361, 385 (2002). The legal requirement of a duty to disclose generally focuses on a physician's duty to inform his or her patients *orally* and is not contingent on writing. *See* Canterbury v. Spence, 464 F.2d 772, 780 n.15 (D.C. Cir. 1972). However, several of the empirical studies in the field of informed consent examined written materials provided to patients and/or research subjects with the aim of assessing understandability. "Informed consent" as used in the remainder of this part is not meant to focus on the legal definition, but rather the process of using written materials with a goal of patient understanding.

202. Kenneth D. Hopper et al., *The Readability of Currently Used Surgical/Procedure Consent Forms in the United States*, 123 SURGERY 496, 498 (1998) (finding that the mean grade level of 616 surgical consent forms was 12.6); Lynn J. White et al., *Informed Consent for Medical Research: Common Discrepancies and Readability*, 3 ACAD.

perts have found that nearly one-half of all Americans are minimally literate.[203] In many cases, the readability standards established by the institution exceeded the reader's ability to read by nearly three grade levels.[204] If information given as part of the informed consent process is limited to written form, these studies indicate, in light of national literacy standards, that patients do not understand to what they are consenting.[205]

In addition to a stark disparity between consent language readability and patient skills, there is evidence that patients are not actually informed when they consent to certain procedures. For example, one study of surgery participants found that nearly half of consenting patients did not actually understand the risks associated with the procedure.[206] Another study of patients agreeing to be research participants found that patients could not correctly answer questions about the study.[207] Interestingly, many patients report satisfaction with the informed consent process—indicating that

EMERGENCY MED. 745, 746, 748 (1996) (finding that forms from three different Midwest hospitals had an average readability grade of 13.8).

203. *See* National Adult Literacy Survey 1992, *available at* http://www.nifl.gov/nifl/facts/NALS.html (on file with author, last visited Dec. 6, 2004); *see also* Terry C. Davis et al., *The Gap Between Patient Reading Comprehension and the Readability of Patient Education Materials*, 31 J. FAM. PRAC. 533, 535 (1990) [hereinafter Davis et al., *Gap*] (finding that patient reading levels at community clinics (5th grade), university clinics (average 6th grade), and in private health settings (10th grade) were below the reading level of the written materials (11th to 14th grade)).

204. *See* Davis et al., *Gap*, *supra* note 203; L. William Katz & Helen Osborne, *Simplicity Is the Best Medicine for Compliance Information*, 17 PATIENT CARE MGMT. 7, 7 (2002); Michael K. Paasche-Orlow et al., *Readability Standards for Informed-Consent Forms as Compared with Actual Readability*, 348 NEW ENG. J. MED. 721 (2003).

205. *See* Terry C. Davis et al., *Parent Comprehension of Polio Vaccine Information Pamphlets*, 97 PEDIATRICS 804 (1996) [hereinafter Davis et al., *Polio Vaccine*] (arguing that readability scores of vaccination pamphlets cannot be relied upon to predict comprehension because many of the study participants had actual comprehension below their reading grade level). Mariner and McArdle argue that readability alone is an inadequate means of assessing comprehension but must be considered in connection with "the effect of culture and experience on a patient's comprehension, the value ascribed to the concept of informed consent, and the circumstances in which the document is distributed." Mariner & McArdle, *supra* note 199, at 73.

206. B.M. Stanley et al., *Informed Consent: How Much Information is Enough?*, 68 AUST. & N.Z. J. SURGERY 788, 789 (1998).

207. Traci Mann, *Informed Consent for Psychological Research: Do Subjects Comprehend Consent Forms and Understand their Legal Rights?*, 5 PSYCHOL. SCI. 140, 142 (1994) (finding that patients who had signed consent forms were only able to answer correctly 60% of specific questions regarding the study and 50% of general questions).

they feel informed, when in fact, further study reveals that their comprehension is actually limited.[208]

Beyond pure readability, cultural factors and patient demographics may also influence the comprehension in the informed consent process. Studies have found that patients who are elderly,[209] lower income, or non-native English speakers[210] are less likely to comprehend informed consent materials.

Training can alleviate some of the problems with consent documents. Research has shown that when researchers are provided with a sample form with explicit writing instructions, many will "produce research informed consents that are clearly superior in comprehensibility" to those produced without such guidance.[211]

The level of patient understanding rises when the information provided is shorter and more concise,[212] or uses story books, a larger typeface, lower reading level, quizzing, disclosing parts rather than all at once,[213] or multimedia presentations,[214] such as videos.[215] Readability of written materials can be improved by having linguistic professionals draft the language, using some best practices such as restructuring the text into a logical sequence, using smaller segments and subheadings, using shorter sentences, and using lay language as opposed to professional language.[216]

208. *E.g.*, Mariner & McArdle, *supra* note 199, at 71.

209. Jeremy Sugarman et al., *Getting Meaningful Informed Consent from Older Adults: A Structured Literature Review of Empirical Research*, 46 J. AM. GERIATRIC SOC'Y 517, 520 (1998) (conducting a meta-analysis of ninety-nine empirical research studies and finding that "[a] substantial number of studies with different populations showed that increased age was related to diminished comprehension.").

210. Mark G. Kuczewski & Patricia Marshall, *The Decision Dynamics of Clinical Research: The Context and Process of Informed Consent*, MED. CARE, Supp. 2002, at v-45, v-49.

211. Sandra J. Philipson et al., *Effectiveness of a Writing Improvement Intervention Program on the Readability of the Research Informed Consent Document*, 47 J. INVESTIGATIVE MED. 468, 475 (1999).

212. Mann, *supra* note 207, at 142.

213. Sugarman et al., *supra* note 209, at 520.

214. Holly B. Jimison et al., *The Use of Multimedia in the Informed Consent Process*, 5 J. AM. MED. INFORMATICS ASS'N 245, 252–54 (1998) (finding that patients thought a multimedia presentation at which participants could proceed at their own rate, utilizing graphics, definitions, and summaries at the beginning and end, was more understandable than a paper form).

215. *See* B.S. Spunt et al., *An Interactive Videodisc Program for Low Back Pain Patients*, 11 HEALTH EDUC. RES. 535, 537 (1996) (finding that viewing the video helped more patients decide whether to proceed with treatment); Sugarman et al., *supra* note 209, at 520.

216. Else Bjørn et al., *Can the Written Information to Research Subjects be Improved?—An Empirical Study*, 25 J. MED. ETHICS 263, 264–67 (1999) (finding that

Lowering the reading level and adding graphics "ma[kes] the consent document easier to read and less frightening to the participants but d[oes] not [necessarily] improve comprehension of the elements within it."[217]

The research on the efficacy of informed consent suggests that a disclosure-based system does not always adequately inform the intended audience. Despite a requirement that plain language be used in NPPs, there is a possibility that the documents will be written at a higher grade level than the average health care consumer can read. And even when written at the proper level, comprehension is not guaranteed.

> [T]he Department agrees that it will not be easy for every individual to understand fully the information in the notice, and acknowledges that the onus of ensuring that individuals have an understanding of the notice should not be placed solely on health care providers. The Rule ensures that individuals are provided with a notice in plain language but leaves it to each individual's discretion to review the notice and to initiate a discussion with the covered entity about the use and disclosure of his or her health information or the individual's rights.[218]

While research shows that through proper training, guidance and the provision of samples, authors of disclosure documents can improve the document's readability and comprehensibility, HHS provides severely deficient guidance, no training and no samples. Moreover, the research regarding the disconnect between patient satisfaction and perceived comprehension and actual comprehension suggests that recipients of an NPP may be overly confident in their personal knowledge or awareness of their rights with respect to their personal health information privacy. In other words, there may be a gap between what patients believe their rights to be with

---

those techniques improved patients' perceived understanding); Katz & Osborne, *supra* note 204, at 7–9. *But see* Stanley et al., *supra* note 206, at 789–90 (finding that additional verbal, written or verbal and written information did not substantially improve patients' understanding).

217. Terry C. Davis et al., *Informed Consent for Clinical Trials: A Comparative Study of Standard Versus Simplified Forms*, 90 J. NAT'L CANCER INST. 668, 672 (1998).

218. Privacy Rule, 67 Fed. Reg. 53,182, 53,241 (Aug. 14, 2002). The commentary also states, "However, the Department continues to believe strongly that promoting individuals' understanding of privacy practices is an essential component of providing notice to individuals. The Department anticipates that many stakeholders, including the Department, covered entities, consumer organizations, health educators, the mass media and journalists, and a host of other organizations and individuals, will be involved in educating individuals about privacy notices and practices." *Id.*

respect to PHI and what their rights actually are. Such a disparity is particularly problematic if HHS enforcement relies upon individual complaints.

While the analogy to informed consent is instructive, it is imperfect. Informed consent deals with sophisticated medical concepts and terminology, including symptoms, treatments, side effects and the like, virtually unknown to the general public, whereas HIPAA NPP disclosure does not need to contain any technical language or terms of art.[219] That is, the content of the disclosure in informed consent is much more complicated than that which is contained within the NPP, so it may be easier to craft more readable NPPs which may be comprehended by a wider segment of the population.

Nonetheless, the analogy is still helpful. HHS makes it explicit that providers are not responsible for ensuring patient understanding whereas informed consent is premised upon understanding. If patient understanding is lacking in a process designed specifically for understanding, what makes us think that patient understanding will be accomplished in a process that specifically states that understanding is not required? This is especially true in light of research by the American Medical Association, showing that physicians "infrequently had complete discussions of clinical decisions with their patients," where informed consent was required.[220] If a routine practice toward promoting understanding is not followed where it is expected, it is difficult to have faith that practitioners will seek understanding with the HIPAA NPP, where they are not required to do so.

B. Information Overload

The NPP as currently structured requires so much information to be provided at one time that patients are not likely to pay attention to or understand what is being disclosed. As will be explored in this section, the abundance of information required is likely to interfere with people's ability to comprehend the information.

219. On the other hand, a study of patients consenting to have their medical encounters videotaped showed that most consent forms "omit key components of informed consent . . . and are written well above recommended reading levels." Dennis J. Butler, *Informed Consent and Patient Videotaping*, 77 ACAD. MED. 181, 183 (2002). Presumably, like the NPP, highly technical medical terminology is not necessary in a consent for a physician visit to be videotaped.

220. Clarence H. Braddock, III, et al., *Informed Decision Making in Outpatient Practice: Time to Get Back to Basics*, 282 JAMA 2313, 2318–19 (1999).

The psychological theory of information overload posits that humans can be overwhelmed by too much information such that their ability to cognitively process the information declines.[221] "When presented with 'too much' information, consumers may become confused, so that they are unable to effectively and efficiently process the information . . . ."[222] One study of hikers attending to information on a trail bulletin board found that "[a]s information quantity increased, attention per message and retention of message content both declined. The positive effects of exposure to more information were nullified by the negative effects of inadequate attention and retention of information."[223] To cope with this phenomenon, humans tend to screen out some information by selectively attending to other information.[224] However, the average consumer—who may not know how multiple pieces of information in a document relate to one another—may have difficulty knowing to which information to attend.[225] Time pressures upon the consumer during receipt of the information can exacerbate this problem.[226]

The information overload theory suggests that when creating a disclosure-based scheme, policy makers should be attentive to the difference between making information available and the "processability of [that] information," the mode of presentation, and the setting and time constraints within which the information is shared.[227] The NPP is required to have a description and example of the types of uses and disclosures made for treatment, payment

221. *See generally*, ORRIN E. KLAPP, OPENING AND CLOSING: STRATEGIES OF INFORMATION ADAPTATION IN SOCIETY 47–80 (1978).

222. Naresh K. Malhotra, *Reflections on the Information Overload Paradigm in Consumer Decision Making*, 10 J. CONSUMER RES. 436, 438 (1984).

223. David N. Cole et al., *Information Quantity and Communication Effectiveness: Low-Impact Messages on Wilderness Trailside Bulletin Boards*, 19 LEISURE SCI. 59, 69 (1997); *see also* Davis et al., *Polio Vaccine*, *supra* note 205 (finding that "current materials contain an excessive amount of information that most patients do not find useful" and recommending that "[t]he number of concepts per pamphlet should be limited").

224. *See* Jacob Jacoby, *Perspectives on Information Overload*, 10 J. CONSUMER RES. 432 (1984) (arguing that it is the very act of screening out information that protects individuals from becoming overloaded with information); KLAPP, *supra* note 221, at 61.

225. *See* Nancy Lockitch Loman & Richard E. Mayer, *Signaling Techniques that Increase the Understandability of Expository Prose*, 75 J. EDUC. PSYCHOL. 402, 410 (1983).

226. *See* Debra L. Scammon, *"Information Load" and Consumers*, 4 J. CONSUMER RES. 148, 154 (1977).

227. Malhotra, *supra* note 221, at 438 exhibit 1; *see* Jacob Jacoby et al., *Corrective Advertising and Affirmative Disclosure Statements: Their Potential for Confusing and Misleading the Consumer*, J. MARKETING, Winter 1982, at 61, 68 ("The difficulty in-

and health care operations; description of the uses and disclosures for which authorization is not required, with sufficient detail to put the individual on notice of the legal requirements; statements of the individual's rights regarding her PHI; descriptions of the entity's duties with respect to PHI; other stock sections, such as to whom complaints should be addressed, contact information, and information about authorizations and revocation of authorizations; and discussion of more stringent state laws.[228] The vast amount of material required combined with the fact that the NPP is targeted to all audiences, from medically and legally sophisticated patients to highly unsophisticated patients, suggests that the information contained within, if read at all, will be screened out with very little of it comprehended.[229]

Moreover, because a patient is given the information when seeking treatment, there may be environmental factors, such as anxiety about the medical visit, a desire to please an authority figure, time pressure, and others that distract the recipient's attention from this important element of her health care. Because HHS permits the NPP to be given when other consents and authorizations are given, it may be lost in a flurry of paperwork, and more importantly, the patient may be unable, cognitively, to properly attend to this important resource. Again, because HHS relies so heavily on the NPP for the proper protection of health privacy, this result seems unacceptable.

In response to these concerns, HHS permits the notice to be provided in "layered" format, which would allow the entity to provide a shorter notice that "briefly summarizes the individual's rights . . . and a longer notice, layered beneath the short notice, that contains all of the [required] elements . . . ."[230] While layered notice may be an important tool to aid comprehension, it is neither required nor recommended; it is merely permissible.[231] Other than requiring NPP distribution on the date of first treatment, or as soon as practicable in emergency situations,[232] there are no temporal requirements, such as the amount of time a practitioner must

volved in accurately communicating meaning is often underestimated, and regulators would seem to be no exception in this regard.").

228. 45 C.F.R. § 164.520 (2003).

229. In fact, HHS received commentary along these lines during the notice of rulemaking period. Privacy Rule, 67 Fed. Reg., 53,182, 53,242 (Aug. 14, 2002) ("[A] shorter notice would assure that more individuals would take the time to read and be able to understand the information.").

230. Privacy Rule, 67 Fed. Reg. at 53,243.

231. *Id.*

232. *See* 45 C.F.R. § 164.520(c).

permit the patient to review the NPP, or a time delay between distribution of the NPP and treatment, in non-emergent situations, so time pressures may be a factor in patients' comprehension.

While much of the empirical research on information overload has been conducted with consumer advertising and the results may not be immediately applicable to health information, the research regarding cognitive ability and comprehension can still be helpful. As shown above in informed consent practice, longer forms with more information do not enhance understanding. If this is true in the informed consent area, and true in the general consumer area, it may also be true in the health information privacy area.

C. Inference Building

There is a complex body of psychological literature dealing with the mental processes of cognition, particularly with respect to understanding of written text—much of which is beyond the scope of this article. However, one of the generally accepted principles of cognition is that when people read, they draw inferences from both the written text and from what they know to exist in the world around them.[233] These inferences help to inform their understanding. Because the NPP is structured only to disclose the *permissible* uses and disclosures of PHI, it presumes that health care consumers are aware of the various ways—permissible and impermissible—in which health care entities use PHI. This presumption may be inaccurate.

When reading a sentence, a person seeks clarity by drawing inferences from what has been read previously or from what is known from prior experience. If the reader is unable to gain clarity from what has been read already, the reader "can draw on his or her background knowledge to fill in the missing . . . content."[234] "[R]eaders need to know . . . how the information 'fits' with other pieces of information they have or need."[235] It barely needs saying that in order for people to be able to draw on their background knowledge, there must be knowledge in the background.

Arguably, the average person is unaware of the multitude of ways that her protected health information may be used and dis-

233. *See* Paul van den Broek et al., *A "Landscape" View of Reading: Fluctuating Patterns of Activation and the Construction of a Stable Memory Representation*, MODELS OF UNDERSTANDING TEXT 165, at 166–67 (Bruce K. Britton & Arthur C. Graesser eds., 1996).

234. *Id.* at 167.

235. Mary E. Vaiana & Elizabeth A. McGlynn, *What Cognitive Science Tells Us about the Design of Reports for Consumers*, MED. CARE RES. & REV., Mar. 2002, at 3, 6.

closed by a health care entity on a regular basis.[236] If a person does not know all or most or even some of the different ways in which PHI is used and disclosed, and if she is told in the NPP only the permissible uses and disclosures, she will not have a frame of reference or background knowledge from which to draw the inference of the ways in which the PHI *may not* be used and disclosed. Without this inference, not only will comprehension of the NPP be reduced, but people will be unable to reliably enforce the Privacy Rule, because they may not know where to look for improper uses and disclosures.

Education directed at patient awareness of the multitude of ways that their information is used is a crucial step toward enhancing comprehension of patient rights with respect to their personal health information. HHS acknowledges as much in the preamble.[237] Yet the Privacy Rule contains no provision—other than the NPP—for educating the public regarding their health information uses and disclosures.[238]

IV.
RECOMMENDATIONS

While the Privacy Rule is an important first step toward health information privacy, the mechanism for informing the public regarding its rights—the NPP—does not go far enough to ensure the goals of the Privacy Rule. This article has discussed four critiques of the regulations regarding the Notice of Privacy Practices. First, the regulations require the NPP to be written in plain language, but provide no guidance as to how to do so or how to evaluate whether it has been achieved.[239] Second, a mere requirement of plain language is inadequate to ensure that the notice is comprehensible, especially given HHS's message to providers that they do not have to ensure that patients understand. Third, too much information is required in the NPP, so that health care consumers are likely to be overloaded by its volume and therefore unlikely to adequately at-

236. In light of the speed and ease with which information may be shared, the number of people and settings in which PHI may be disclosed is not surprising. For example, health care students in training often take PHI out of the health care setting on their Personal Data Assistants. The 2000 Privacy Rule preamble identifies a myriad of ways in which health information flows and recognizes that "much of this sharing of information is done without the knowledge of the patient involved." Privacy Rule, 65 Fed. Reg. 82,462, 82,466 (Dec. 28, 2000).

237. *See supra* note 182.

238. For more discussion of the possibilities of an awareness campaign, see *infra* Part IV.

239. *But see supra* text accompanying note 172.

tend to its content. And fourth, the required elements of the NPP focus on what covered entities may do, but no provision is included for educating the public regarding what entities may not do. This section recommends some improvements to the NPP and the Privacy Rule, with the goal of enabling or empowering individuals to be actively involved in protecting their health information privacy.

A written notice with no specifications regarding format, style, font, and headings is inadequate. Proper headings help readers organize and attend to written content. Headings function as signals which "direct attention toward conceptual information and away from the primacy/recency information in a passage . . . . [and] encourage[ ] the reader to build a coherent learning" from the passage.[240] Other than the introductory heading, the Privacy Rule does not require the information contained within the NPP to be organized in any particular manner. While the information requirements lend themselves to a coherent organization—patient's rights, contact information, etc.—the regulations do not require the use of any such headings. Because it could improve coherence and hence comprehension to organize the material with headings and fonts clearly indicating those headings,[241] and because it is a simple change that could enhance the NPP significantly, HHS should require certain formatting. Moreover, font size and other layout requirements would counteract any incentive on the provider's part to save money by making the notice smaller or to fit the notice on fewer pages.

The purely text-based NPP could be improved through the use of multimedia. As research in other settings has shown, audiovisual information has been found to improve recall of the information and patient satisfaction with the process.[242] Including pictures and having a congruent picture-verbal design increases understanding.[243] "Decision aids," such as brochures with pictures, have been found to produce greater knowledge of the material, less conflict

240. Lockitch Loman & Mayer, *supra* note 225, at 410 (finding that without signals, readers tend to recall the first and last things they read, *i.e.*, the primacy/recency effect).

241. *See* Vaiana & McGlynn, *supra* note 235, at 6–7 (identifying the text features of user-friendly documents). Vaiana and McGlynn argue that headings, lists, and paragraphs help readers organize the information, and features of type such as font, boldness and color help cue the important information. *Id.*

242. Raich et al., *supra* note 200, at 440.

243. Sujit S. Sansgiry & Paul S. Cady, *An Investigative Model Evaluating How Consumers Process Pictorial Information on Nonprescription Medication Labels*, HEALTH MARKETING Q., Vol. 14(4) 1997, at 71, 81–84 (studying consumer response to medication product labels).

for the decision-maker, and more involvement of the patient in making the decision.[244] In light of this experience, it seems clear that the understandability of text-only notice can be improved by the use of graphics, color, pictures, and other media. For example, instead of simply writing that the "entity may not disclose such information," a picture of a person's mouth as if they were talking about health information or a cartoon with a talk bubble and a big slash through it to indicate no talking could be used to supplement the written text. Multimedia could be used as a source of examples, such as video segments showing skits demonstrating the proper usage of PHI. Such multimedia techniques could be reviewed by a patient at her own pace without the pressure of standing before a nurse or receptionist.

No oral explanation is required and often none is given upon delivery of the NPP. While including an oral explanation component may introduce more variables, making enforcement more difficult, an oral explanation will most likely aid in comprehension.[245] If the provider initiated an oral conversation, the patient is invited to engage in conversation regarding her information privacy, which is part of the goal of the Privacy Rule.[246] At the very least, a provider could inquire whether the patient had any questions upon receiving the NPP. Even this simple invitation to discussion is not required by the Privacy Rule as it is currently composed.

The problem of information overload can also be mitigated through oral explanations by signaling health care consumers to which information they should attend. More education and layered notice as discussed in Part III.B can also alleviate the information overload problem.

As considered in Part II.B, more specific requirements regarding the assessment of plain language should be included. Whether through a specific measure of whether an NPP is written in plain

244. Margaret Holmes-Rovner & Celia E. Wills, *Improving Informed Consent: Insights from Behavioral Decision Research*, 40 MED. CARE v-30, v-34–v-35 (Supp. 2002). *See also* Davis et al., *Polio Vaccine*, *supra* note 205 ("simple, short, colorful materials written at . . . lower [grade] levels actually may be more appealing to all audiences, and that even simpler materials with more instructional graphics, coupled with oral instruction, may be needed for [patients] reading below a seventh grade level").

245. Davis et al., *Polio Vaccine*, *supra* note 205.

246. Privacy Rule, 67 Fed. Reg. 53,182, 53,240 (Aug. 14, 2002) ("The notice acknowledgement process is intended to provide a formal opportunity for the individual to engage in a discussion with a health care provider about privacy. At the very least, the process is intended to draw the individual's attention to the importance of the notice."); *see also supra* note 177 and accompanying text.

language or a more subjective measure, providers need to be able to know if they have achieved plain language.

Finally, HHS should enhance its Privacy Rule and its reliance on the NPP through a comprehensive educational campaign to raise awareness of health information privacy rights and responsibilities. While this is suggested in the commentary to the rule, there is no provision for such educational programs.[247] HHS could undertake such initiatives and/or could engage in grant-making to entities dedicated to health literacy to encourage more comprehensive health information education.[248] Examples might include the creation of brochures, videos, a website or training modules to be included in certain basic life skills classes. Additionally, public awareness campaigns through the media would enhance individuals' awareness of their rights.

CONCLUSION

The HIPAA Privacy Rule is a necessary element of the federal initiative toward administrative simplification in the field of health care. In striking a balance between strict privacy protection for individuals and ease of administration for the health care industry, HHS has created a regulation that is only satisfactory if viewed as a starting point. The critiques and recommendations discussed above are crucial if the nation is to achieve a policy of protecting *all* individuals' private health information.

247. HHS provides training geared toward covered entities, but not for the healthcare consumer. *See* http://www.cms.hhs.gov/hipaa/hipaa2/education/default.asp (last visited November 22, 2004).

248. *See, e.g.*, Kathleen K. Wilson, INSTITUTE ON FAMILY AND NEIGHBORHOOD LIFE AT CLEMSON UNIVERSITY, PROMOTING HEALTH LITERACY (2001).