UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 77 | Number 1 Article 8

11-1-1998

Enacting a Health Information Confidentiality Law: Can Congress Beat the Deadline

Bartley L. Barefoot

COMMENT

Enacting a Health Information Confidentiality Law: Can Congress Beat the Deadline?

I. INTRODUCTION

Americans are worried about their privacy. Surveys consistently indicate widespread concern about access to and use of personal information by others,[1] with the privacy of health-related information the object of particular concern.[2] Unfortunately, the public has good reason to be worried. Health-related information has become a valuable commodity used for a vast number of purposes unrelated or only indirectly related to the provision of care; many Americans would be shocked to learn the breadth of individuals and organizations with access to their most sensitive information.[3] At the same time, access to health information is critical for the efficient delivery of and payment for quality care, as well as for numerous other activities that benefit society.[4] Currently, use of health information is governed by a patchwork of federal and state laws that provides inconsistent and often ineffectual privacy protections and that inhibits the increasingly computerized flow of data.[5] In recent years, consensus has developed that a uniform, comprehensive federal health confidentiality law should replace this patchwork of statutes and cases.[6] Despite this consensus, each attempt to enact such a law during the past eighteen years has failed, largely because

---

1. Equifax, Inc., one of the nation's largest consumer information agencies, has commissioned Lou Harris & Associates to conduct a survey of attitudes toward information privacy issues each year since 1990. The percentage of respondents who were "very" or "somewhat" concerned about threats to personal privacy was 83% in 1994, EQUIFAX/HARRIS CONSUMER PRIVACY SURVEY (1994), and 82% in 1995, *id.* (1995). In 1995, 80% of respondents agreed that "consumers have lost all control over how personal information about them is circulated and used by companies." *Id.* (1995).

2. In a 1993 Equifax/Harris survey focusing specifically on privacy of health-related information, 85% of the respondents said that protecting the confidentiality of health data is "absolutely essential" or "very important." EQUIFAX/HARRIS HEALTH CARE INFORMATION PRIVACY SURVEY (1993).

3. *See infra* note 49 and accompanying text.

4. *See infra* notes 25-36 and accompanying text.

5. *See infra* notes 76-170 and accompanying text.

6. *See infra* notes 182-85 and accompanying text.

privacy advocates and members of the health care industry cannot agree on numerous points[7] concerning this extraordinarily complex issue.[8] In 1996, Congress enacted an August 1999 deadline for passage of health confidentiality legislation.[9] If this deadline is not met, privacy rights and confidentiality obligations regarding computerized health data will be determined solely by regulations promulgated by the Department of Health and Human Services ("HHS").[10] If the past serves as any indication, disagreements on several key issues may cause the deadline to pass without congressional action.[11]

This Comment analyzes the current state of the health information confidentiality debate, identifying areas of consensus as well as points of disagreement that must be resolved if Congress is to enact a comprehensive federal health confidentiality law. Part II reviews the privacy risks posed by the growing demand for health information, the reliance on information technology, and the shortcomings of existing federal and state confidentiality laws.[12] Part

7. *See infra* notes 205-31 and accompanying text. In this Comment, the term "privacy advocates" and its permutations refer generally to civil liberties, patients' rights, mental health advocacy, HIV advocacy, and similar organizations. The term "health care industry" and its permutations refer generally to insurers, information processing companies, managed care organizations, and other institutional users of information. The latter term also occasionally encompasses non-health-related users of information, such as law enforcement, who share industry's desire for a less stringent confidentiality law. These terms are generalizations and are not intended to represent the views of every organization. Viewpoints do not necessarily equate with titles. The members of the American Medical Association ("AMA"), for example, are part of the health care "industry," but the AMA's position on many confidentiality issues is closely aligned with that of privacy advocates. *See, e.g.*, Donald J. Palmisano, Testimony on Behalf of the American Medical Association Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 46 (Feb. 18, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) (arguing for a federal law that does not preempt more stringent state confidentiality rules).

8. Republican Congressman Christopher Shays of Connecticut, a sponsor of one health privacy legislative proposal, noted that he was "not prepared for the degree of complexity and the competing interests" that he found when first looking at this issue. *Medical Privacy Protection: Hearing Before the Subcomm. on Gov't Management, Info., and Tech. of the House Comm. on Gov't Reform and Oversight*, 105th Cong. (1998) [hereinafter *Medical Privacy Protection Hearing*] (statement of Rep. Christopher Shays), *available in* 1998 WL 12760503.

9. *See infra* notes 232-35 and accompanying text.

10. *See infra* note 235 and accompanying text.

11. *See infra* notes 205-31 and accompanying text.

12. *See infra* notes 16-170 and accompanying text. For a discussion of health and confidentiality issues generally, see OFFICE OF TECH. ASSESSMENT, PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION (1993) [hereinafter OTA]; Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451 (1995); Lawrence O. Gostin et al., *Privacy and Security of Health Information in the Emerging*

III discusses previous, unsuccessful efforts to enact a federal health confidentiality law, as well as recent activity at the federal level relating to privacy of health information.[13] Part IV focuses on certain issues that have proven particularly difficult and discusses the often divergent perspectives of various interested parties.[14] The Comment concludes with a discussion of several areas in which compromise is critical for passage of meaningful confidentiality legislation before the August 1999 deadline.[15]

II. THE CURRENT STATE OF HEALTH INFORMATION PRIVACY

A. Sensitivity of Health Information

Of all the kinds of personal information, arguably none is more sensitive than health-related information. The contents of patient records held by doctors and other care-givers provide a clear example of both the breadth and the intimate nature of "health-related information." A typical patient record contains demographic information (such as age and race) as well as detailed notes concerning the patient's history of diseases, treatments, medications, and diagnostic tests; family history and results from genetic testing;[16] history of substance abuse, mental illness, or violent behavior; favorite (and dangerous) recreational activities; dietary habits; sexual orientation, sexual activities, and results from tests for sexually transmitted disease; employment status and income; and eligibility for public assistance.[17] The contents of the patient record are not limited, however, to objective test data or information provided by the patient. Medical records also frequently contain the impressions of doctors and nurses, including assessments of a patient's character, personality, and mental state.[18]

The vast amount and scope of information held within these records has led to the suggestion that a medical record contains more highly personal information than any other single document.[19] While

---

Health Care System, 5 HEALTH MATRIX 1 (1995); Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295 (1995).

13. *See infra* notes 171-264 and accompanying text.

14. *See infra* notes 265-530 and accompanying text.

15. *See infra* notes 531-58 and accompanying text.

16. Genetic information is particularly sensitive because it relates not only to present medical conditions but also to the propensity of future conditions. *See* OTA, *supra* note 12, at 28-29.

17. *See id.* at 5, 27-28; Gostin, *supra* note 12, at 490.

18. *See* OTA, *supra* note 12, at 26, 28.

19. *See* PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN

this assertion is subjective, undoubtedly the "modern [medical] record is a warehouse of information."[20] The universe of health-related information is, of course, not limited to patient records held by doctors and hospitals. Varying amounts of personally identifiable health data are also held in the records of thousands of other entities, including employers, insurance companies, government agencies, credit bureaus, licensing and accreditation organizations, as well as held by the media.[21]

No matter the location, the social, psychological, and economic consequences of the unwanted disclosure of health-related information can be devastating.[22] Disclosure can have significant public health consequences as well. If individuals fear that their privacy will not be respected, they are less likely to discuss problems and risky behaviors candidly with their health care provider, thereby increasing the risk of misdiagnosis or inadequate care.[23]

B. The Demand for Health Information

The sensitivity of health information gives rise to a reasonable expectation among patients that it will be held in confidence.[24] This expectation conflicts, however, with the growing demand for information by the health care industry[25]—demand fueled largely by sweeping changes in the way health care is delivered.[26] The days of predominantly freestanding health care providers and insurers are drawing to a close as the health care industry continues to integrate itself, shifting toward a managed care model with networks of providers and payers.[27] As the industry has grown more

---

INFORMATION SOCIETY 282 (1977) [hereinafter PRIVACY COMMISSION].

20. Robert M. Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 N.C. L. REV. 255, 258 (1984).

21. *See* H.R. REP. NO. 103-601, pt. 5, at 70-71 (1994) (Report of the Comm. on Gov't Operations accompanying H.R. 3600); Gostin, *supra* note 12, at 490.

22. *See* Gostin, *supra* note 12, at 490. For some notable examples of the consequences of unwanted disclosure of health-related information, see OTA, *supra* note 12, at 27.

23. *See, e.g.*, Gellman, *supra* note 20, at 257.

24. *See id.*

25. *See* INSTITUTE OF MED., THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE 21 (Richard S. Dick & Elaine B. Steen eds., 1991) [hereinafter COMPUTER-BASED PATIENT RECORD].

26. *See, e.g.*, Gellman, *supra* note 20, at 259-60.

27. *See, e.g.*, *Medical Privacy Protection Hearing*, *supra* note 8 (prepared statement of Charles N. Kahn, III, Chief Executive Officer, Health Insurance Association of America), *available in* 1998 WL 12760470; *The Fair Health Information Practices Act of 1997: Hearings on H.R. 52 Before the Subcomm. on Gov't Management, Info., and Tech. of the House Comm. on Gov't Reform and Oversight*, 105th Cong. 20 (1997) [hereinafter

interconnected, the ability to access and share data easily and quickly has assumed heightened importance.[28] Providers, insurers, and other entities affiliated with treatment and payment in the modern health care system use health information for a wide variety of purposes, including not only the actual delivery of and payment for care but also disease management programs[29] and quality of care assessments.[30]

The desire to control health care spending is one of the primary forces behind these changes in the health care industry. Health plans and health care administrators conduct utilization reviews to determine how their resources are used, what treatments are most cost-effective, and how expenditures can be reduced.[31] These reviews frequently involve examinations of significant numbers of personally identifiable health records.[32] It is now common practice for managed care organizations, such as health maintenance organizations ("HMOs"), to demand detailed patient information from providers before approving additional treatment.[33] Payers are also investigating claims for waste and fraud with increasing vigilance.[34] Finally, the federal government's involvement in payment for health care has added to the demand for patient records.[35] Like commercial

---

Hearings on H.R. 52] (statement of Sherine Gabriel on behalf of the Health Care Leadership Council). One example of the integration movement is Intermountain Health Care ("IHC"). As of February 1997, IHC operated 23 hospitals and 33 clinics and offered health insurance plans to more than 350,000 persons in three states. *See* John T. Nielsen, Testimony on Behalf of the American Hospital Association Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 42 (Feb. 18, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Nielsen Testimony].

28. *See, e.g., Medical Privacy Protection Hearing, supra* note 8 (prepared statement of Charles N. Kahn, III, Chief Executive Officer, Health Insurance Association of America), *available in* 1998 WL 12760470; David L. Larsen, Testimony on Behalf of the American Association of Health Plans Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 7-8 (Feb. 3, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Larsen Testimony].

29. For example, many managed care organizations use "care process models" to determine if clients are at risk for certain conditions and, if so, to ensure they receive preventive screening. *See* Larsen Testimony, *supra* note 28, at 19-20.

30. *See id.*

31. *See* COMPUTER-BASED PATIENT RECORD, *supra* note 25, at 21-22.

32. *See, e.g.*, Larsen Testimony, *supra* note 28, at 7-8.

33. *See id.* For example, HMOs and health plans routinely interview mental health providers by phone to ascertain whether a patient really requires treatment, and some send their own nurses into hospitals to review patient charts. *See* Craig S. Palosky & Doug Stanley, *Privacy Lost*, TAMPA TRIB., Feb. 16, 1997, at 1-Nation/World.

34. *See* Gellman, *supra* note 20, at 259-60.

35. *See id.* at 260-61. The Medicare program is the nation's largest third-party payer for health care treatment and services. *See* MALCOLM K. SPARROW, LICENSE TO STEAL:

third-party payers, the government reviews large numbers of patient records in an effort to combat waste and fraud in its Medicare and Medicaid programs.[36] In sum, some level of access to and sharing of patients' health information is an essential ingredient in the modern health care system.

Payers and providers are not, however, the only groups who use personally identifiable health information. The health record has become such a "rich repository" of valuable information that organizations not directly involved in delivering or paying for care also seek its contents.[37] These secondary users include public health organizations, medical and social science researchers, employers, government agencies, educational institutions, law enforcement, credit bureaus, the judicial system, accrediting and licensing organizations, and the media.[38] Individuals may consent to the use of their health information by secondary users, but under current law consent is often not required and, in fact, not obtained.[39] Public health, law enforcement, and other government agencies, for example, can obtain health information without consent through means prescribed by law.[40] Other secondary users, particularly private companies, purchase personally identifiable health information from many willing sellers.[41] This "outward flow of

---

WHY FRAUD PLAGUES AMERICA'S HEALTH CARE SYSTEM at xiii (1996).

36. *See* Gellman, *supra* note 20, at 260-61. As of February 1997, approximately 300 Federal Bureau of Investigation agents worked specifically in health care fraud investigations. *See* Neil Gallagher, Deputy Assistant Director of the Criminal Investigative Division, Testimony on Behalf of the Federal Bureau of Investigation Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 22 (Feb. 18, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Gallagher Testimony]. The Bureau had approximately 2000 health care fraud investigations pending at that time. *See id.*

37. H.R. REP. NO. 103-601, pt. 5, at 70 (1994).

38. *See id.* at 70-71 (citing AMERICAN MED. RECORDS ASS'N, CONFIDENTIALITY OF PATIENT HEALTH INFORMATION: A POSITION STATEMENT OF THE AMERICAN MEDICAL RECORDS ASSOCIATION 5-6 (1977), *reprinted in Privacy of Medical Records: Hearings Before a Subcomm. of the House Comm. on Gov't Operations*, 96th Cong. 326-27 (1979)). The American Medical Records Association is now known as the American Health Information Management Association ("AHIMA").

39. *See* OTA, *supra* note 12, at 31.

40. For example, law enforcement officials can obtain patient records without consent if they have a subpoena or search warrant. *See infra* notes 414-23 and accompanying text.

41. *See* H.R. REP. NO. 103-601, at 71-74 ("[T]here is a demand for health data about identified individuals and . . . there are companies that will collect and sell data to fill that demand."). Information processing companies, which manage patient information for providers and payers, are a primary source of the health information available for sale. *See* OTA, *supra* note 12, at 30-31.

information"[42] is widespread, growing, and yet largely unknown to the average patient.[43]

For many of these secondary users, personally identifiable health information is a valuable tool in the decisionmaking processes of "societal gatekeeping functions."[44] Medical information is used to determine whether an individual will obtain insurance coverage, receive a marriage license, obtain a driver's license, secure employment, retain existing employment, or even obtain credit.[45] The presence of "negative" information in a health record may affect the individual's ability to participate in such basic activities.[46]

Other secondary users obtain health information for the direct marketing of products and services. Recognizing a "strong commercial incentive" to collect health information, marketing companies compile and sell lists of thousands or even millions of individuals with particular health conditions.[47] Pharmaceutical manufacturers and makers of health and beauty products are frequent users and purveyors of such lists.[48] The commercial appeal

42. OTA, *supra* note 12, at 44.

43. *See* Gellman, *supra* note 20, at 261 ("The value of medical information for uses outside the medical treatment and payment system has not been popularly recognized, and even medical professionals are largely unaware of the many uses to which the information may be put.").

44. PRIVACY COMMISSION, *supra* note 19, at 281. The phrase "societal gatekeeping functions" refers to "the use of recorded information to determine whether individuals should be allowed to enter into different types of social, economic, and political relationships, and if so, under what circumstances." *Id.* at 281 n.18.

45. *See* OTA, *supra* note 12, at 29-30; PRIVACY COMMISSION, *supra* note 19, at 281; Gostin, *supra* note 12, at 490. The Medical Information Bureau ("MIB") serves as the "credit bureau" of the life and health insurance industries. MIB maintains medical history files on approximately 15 million Americans and holds these files for seven years. More than 700 life and health insurers throughout North America consult these files as part of the underwriting process. *See* OTA, *supra* note 12, at 32-33.

46. *See* OTA, *supra* note 12, at 29-30.

47. *See* H.R. REP. NO. 103-601, pt. 5, at 71-74 (1994). For a discussion of privacy issues and direct marketing, see Kathleen A. Linert, Note, *Database Marketing and Personal Privacy in the Information Age*, 18 SUFFOLK TRANSNAT'L L. REV. 687 (1995).

48. For example, as of 1994, Johnson & Johnson maintained for sale a list of five million women who suffer from incontinence. *See* H.R. REP. NO. 103-601, at 73 (citing *The Fair Health Information Practices Act of 1994: Hearings on H.R. 4077 Before the Subcomm. on Info., Justice, Transp. and Agric. of the House Comm. on Gov't Operations*, 103d Cong. 372 (1994) [hereinafter *Hearings on H.R. 4077*] (statement of Professor Paul Schwartz)). Pharmacy chains work with pharmaceutical manufacturers to identify individuals with particular medical conditions and then market drug therapies to these individuals. *See* Palosky & Stanley, *supra* note 33, at 1-Nation/World. Following intense public criticism, CVS drug stores and Giant Food grocery stores recently abandoned such programs. *See* Chris Reidy, *CVS Hit with Class-Action Suit over Mailings*, BOSTON GLOBE, Mar. 26, 1998, at C1. CVS and Giant shared lists of customers with Elensys, Inc., which mailed letters tailored to particular medical conditions—the cost of which was

of health-related information is so strong that even organizations that might otherwise be considered "pro-patient" traffic in it.[49] Under current law, these activities are often legal.[50]

C. *Impact of Computerization on Privacy*

Concurrent with the integration of treatment and payment and the increasing demand for information is a growing reliance on technology, which the health care industry views as a means for improving the delivery of care while reducing costs.[51] Central to this effort is a movement toward computerized medical records and the automated storage and transfer of personal health information.[52] Although most health information is still recorded on paper,[53] the shift to computer-based information systems is well under way.[54] The health care industry envisions a future of computerized records in which each individual will have a single, paperless record containing all of his health-related information accumulated from birth until death.[55] This longitudinal record will be stored in databases and shared with authorized users through health data networks linking providers, hospitals, health plans, and other entities.[56] These

---

underwritten by pharmaceutical manufacturers such as Glaxo Wellcome—to the customers encouraging them to purchase medications manufactured by those companies. *See id.*

49. *See* Palosky & Stanley, *supra* note 33, at 1-Nation/World (describing a magazine published for HIV-positive persons that rents its subscription list to direct marketers).

50. *See* H.R. REP. NO. 103-601, at 72-74; OTA, *supra* note 12, at 31.

51. *See, e.g.*, Nielsen Testimony, *supra* note 27, at 42-43.

52. *See, e.g.*, OTA, *supra* note 12, at 6-11.

53. *See* Gostin, *supra* note 12, at 457.

54. Several examples illustrate how technology is already used in the storage and movement of health-related information. Of the 3.5 billion health care payment claims processed in 1994, 1.3 billion (36%) were transmitted electronically. *See Medical Records Confidentiality Act of 1995: Hearings on S. 1360 Before the Senate Comm. on Labor and Human Resources*, 104th Cong. 107 (1995) [hereinafter *Hearings on S. 1360*] (statement of the Association for Electronic Health Care Transactions). Revco Drug Stores, operating in 17 states, electronically links its stores with corporate headquarters and with third-party payers to facilitate filling prescriptions. *See* Robert Thompson, Prepared Statement on Behalf of the National Association of Chain Drug Stores Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 1-2 (Feb. 4, 1997) (unpublished statement, on file with the *North Carolina Law Review*) [hereinafter Thompson Statement]. Revco maintains a centralized database of records so that any of its pharmacists can pull up a customer's medication history. *See id.* Similarly, information technology companies are developing computerized network systems for managed care organizations and health data networks for entire communities. *See, e.g., Hearings on H.R. 4077, supra* note 48, at 325-26 (statement of Dr. Richard Barker, International Business Machines ("IBM")).

55. *See* COMPUTER-BASED PATIENT RECORD, *supra* note 25, at 44.

56. *See id.* at 51-52.

electronic linkages will collectively form a national "health information infrastructure," facilitating the seamless transfer of patient information among data users.[57]

Computerization of health information purportedly offers several advantages over a paper-based information system, including enhanced administrative efficiency,[58] more effective outcome and cost assessment, and improved delivery of care.[59] Commonly cited examples of improvements in care include the ability of any emergency room to access crucial patient history information instantly,[60] a reduction in tests that patients must repeat because past results cannot be located,[61] and the ability of doctors practicing in a managed care network to share patient information.[62] Another oft-cited advantage is the enhanced security that computerization can provide for health-related information such as patient records.[63] Unlike paper-based record systems, computerized systems include controls designed to limit access to authorized persons and to record the electronic movements of these persons when reviewing patient records; although not foolproof, these security features can reduce

57. *See id.* at 50-54; OTA, *supra* note 12, at 6-10. Congress has stated its support for the development of a national health information infrastructure. *See* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C.A. § 1320d, Historical and Statutory Notes (West Supp. 1998) (Purpose of Administrative Simplification). In addition to facilitating the movement of traditional patient records, advances in technology have furthered the practice of telemedicine. For a discussion of privacy concerns related to telemedicine, see Christina M. Rackett, Note, *Telemedicine Today and Tomorrow: Why "Virtual" Privacy Is Not Enough*, 25 FORDHAM URB. L.J. 167 (1997).

58. Administrative expenses, primarily paper-based claims processing, account for approximately 19-24% of health care expenditures. *See* Gostin, *supra* note 12, at 480 (citing Steffie Woolhander & David U. Himmelstein, *The Deteriorating Administrative Efficiency of the U.S. Health Care System*, 324 NEW ENG. J. MED. 1253, 1255-56 (1991)). Some commentators believe that computerization will result in cost savings. *See, e.g.*, Schwartz, *supra* note 12, at 305 ("Information technology may offer the last best hope to control health care costs. It renders accessible to external observation and supervision the enormous amount of data involved in diagnosing, treating, and billing patients. The potential cost savings from greater use of data processing in health care are enormous."). *But see* SPARROW, *supra* note 35, at 122-40 (arguing that any cost savings achieved by computerization will be offset by a corresponding increase in fraudulent claims for treatment).

59. *See* Schwartz, *supra* note 12, at 305-06. For a more complete discussion of the reasons advanced for the computerization of health information, see COMPUTER-BASED PATIENT RECORD, *supra* note 25, at 2-3, 24-26; OTA, *supra* note 12, at 6-11; Gostin, *supra* note 12, at 470-84.

60. *See* Gostin, *supra* note 12, at 477.

61. *See Hearings on H.R. 52*, *supra* note 27, at 78 (statement of AHIMA).

62. *See, e.g.*, Larsen Testimony, *supra* note 28, at 8.

63. *See* Gostin, *supra* note 12, at 492.

the risk of unauthorized access to information.[64]

While computerization may offer significant advantages, it also poses a threat to individuals' privacy.[65] Computerization facilitates the creation of networks connecting large databases containing health-related information on thousands or even millions of persons.[66] These networks allow potentially large numbers of authorized users to access these data from multiple locations, reducing the individual's ability to control the flow of her health-related information.[67] Computers may also allow these users to link data sets intended to remain separated, so that otherwise non-identifiable information may be combined to identify an individual.[68] Furthermore, no electronic safeguard can absolutely guarantee that computerized data will not be stolen or altered.[69] Finally, many observers believe that the ease with which computers permit transfer and analyses will only fuel the already insatiable demand for health-

64. *See* OTA, *supra* note 12, at 11-12. Access may be controlled through the use of passwords and user-specific menus that authorize users to see only those parts of the patient record they have a legitimate reason to see. *See id.* at 11. Audit trails can track the electronic movements of users to reveal patterns of improper behavior on the system. *See id. But see infra* text accompanying note 69 (noting that such safeguards are not foolproof).

65. *See* Gostin, *supra* note 12, at 493.

66. Thousands of computerized databases containing health-related information already exist, some of them quite large. For example, the Medical Information Bureau maintains such a database. See *supra* note 45 for background on MIB. The MIB database likely pales in comparison, however, with the U.S. Medicare claim reimbursement system, which may constitute "the largest collection of health databases in the world" storing vast amounts of personally identifiable information. WILLIAM W. LOWRANCE, PRIVACY AND HEALTH RESEARCH: A REPORT TO THE U.S. SECRETARY OF HEALTH AND HUMAN SERVICES 19 (1997). For a more complete discussion of the variety of public and private health databases in existence, see Gostin, *supra* note 12, at 463-69.

67. *See* Gostin, *supra* note 12, at 492-93. Commentators generally agree that access by authorized individuals—not outside "hackers"—poses the greatest threat to the security of health information. *See* OTA, *supra* note 12, at 11-12. Ease of access is, however, one of the principal arguments for computerization. *See* Gostin, *supra* note 12, at 493. The list of users who would likely have access to computerized patient records is very large, *see* COMPUTER-BASED PATIENT RECORD, *supra* note 25, at 31-33, thus increasing the likelihood that patient information will be given or sold to unauthorized parties, *see* Gostin, *supra* note 12, at 488.

68. *See* OTA, *supra* note 12, at 37. In some information storage schemes, health-related records are stripped of all identifying data (e.g., name, address, social security number), and these data are stored separately. The purpose of this system is to prevent users from determining the identity of any record subject. In a computerized environment, the possibility exists that a sophisticated user, authorized or otherwise, could link the two sets of data to produce personally identifiable information. *See* Gostin, *supra* note 12, at 494.

69. *See* OTA, *supra* note 12, at 37.

related information.[70]

In sum, the demand for health-related information and the concurrent reliance on technology pose a significant policy dilemma. Accurate and timely information is a necessary component of a well-functioning health care system.[71] Computerization promises to facilitate the flow of data among care-givers, payers, and others and to reduce the cost of transfer and storage of such data.[72] The availability of this information allows providers to deliver appropriate care and permits the study of best practices, cost analysis, and other benefits.[73] At the same time, however, the demand for information by so many parties and the ease with which computerization allows these parties to obtain this information necessarily result in a reduction of personal privacy.[74] The potentially harmful social and economic consequences of this intrusion mean that society must strike a balance between competing health care and privacy interests.[75]

D. Current Legal Protections for Confidentiality of Health Information

Unfortunately, our nation has been unable to strike such a balance. Neither statutory nor case law at the federal or state levels offers significant, comprehensive protection for the privacy of all health-related information.[76] This glaring omission is compounded by the failure of many of these laws to keep pace with advances in technology; existing laws are often based on increasingly antiquated notions of a paper-based health information system.[77] A review of the current legal framework reveals that our health-related information receives inconsistent protection that does not take into account changes in the health care industry, the growing secondary use of health information, or the impact of computerization.[78]

---

70. *See id.* at 18.

71. *See* Gostin, *supra* note 12, at 451-52.

72. *See supra* notes 51-64 and accompanying text.

73. *See supra* notes 28-36 and accompanying text.

74. *See* Gostin, *supra* note 12, at 489.

75. *See id.* at 515-16; *see also Protecting Our Personal Health Information: Privacy in the Electronic Age: Hearings Before the Senate Comm. on Labor and Human Resources*, 105th Cong. 6 (1997) [hereinafter *Privacy in the Electronic Age Hearings*] (statement of Donna Shalala, Secretary of HHS) (noting that privacy principles should be "weighed against . . . our public responsibility to support national priorities, public health, research, quality care, and our fight against health care fraud and abuse").

76. *See, e.g.*, Schwartz, *supra* note 12, at 310.

77. *See, e.g.*, OTA, *supra* note 12, at 15.

78. *See infra* Part II.D.1-3.

1. Statutory Protections at the Federal Level

Unlike its European counterparts, the United States has developed a piecemeal approach to information privacy protection.[79] No overarching federal law protects the privacy of information; rather, Congress has enacted privacy laws on an ad hoc basis.[80] This approach has led to separate federal privacy laws governing the collection, use, and disclosure of credit information,[81] financial records,[82] student records,[83] cable television subscriber information,[84] and video rental records.[85] Information concerning individuals treated in federally funded or regulated drug and alcohol dependency programs also receives protection.[86] To the extent that health-related information is included in any of these sources, it receives some form of federal protection. No comprehensive federal law exists, however, for the protection of all health-related information regardless of its source.[87]

Even the most comprehensive federal privacy law, the Privacy Act of 1974,[88] offers limited protection for health information. The Act governs the collection, use, and dissemination of information maintained only by federal government agencies and other institutions operated by the federal government or pursuant to federal contract.[89] Most health-related information, however, is held by private entities who are not covered by the Act.[90] The Act is also

79. *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500 (1995). The members of the European Union have agreed to a comprehensive scheme designed to protect the privacy of all personal data regardless of subject matter. *See infra* notes 237-42 and accompanying text.

80. *See* Reidenberg, *supra* note 79, at 500.

81. *See* Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (1994).

82. *See* Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1994).

83. *See* Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1994).

84. *See* Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1994).

85. *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994). This act was passed in response to the release of Judge Robert H. Bork's video rental record during hearings concerning his nomination for the Supreme Court. *See House OKs Video Privacy Protection Bill*, L.A. TIMES, Oct. 20, 1988, pt. I, at 2.

86. *See* 42 U.S.C. § 290dd-2 (1994).

87. *See* Robert M. Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 VILL. L. REV. 129, 136 (1996). That video rental records receive more protection at the federal level than health-related information is frequently noted by those who question the current state of affairs. *See, e.g., Privacy in the Electronic Age Hearings*, *supra* note 75, at 4 (statement of Donna Shalala, Secretary of HHS).

88. 5 U.S.C. § 552a (1994).

89. *See id.* § 552a(a)(1), (m)(1); OTA, *supra* note 12, at 42.

90. *See* Schwartz, *supra* note 12, at 315.

riddled with exceptions.[91] For example, while federal agencies are generally obligated to obtain consent before disclosing personally identifiable information, at least twelve exceptions to this requirement exist,[92] most notably an exception for "routine use" disclosures.[93] Federal agencies have interpreted the routine use exception so broadly that individuals are effectively unable to control the flow of information through the power of consent.[94] And, like so many other privacy laws, the Act has not kept pace with technology; designed for a world of paper-based information systems, it does not contemplate databases of millions of records instantaneously accessible from remote locations.[95] While its purpose and provisions were at the vanguard of privacy protection at its inception, the Privacy Act has recently been labeled one of the "most outdated" national privacy laws in the world.[96]

2. Constitutional Right to Privacy

Whatever right to privacy the U.S. Constitution guarantees has also been of limited benefit to the protection of health information.[97] Like the Privacy Act, the right to privacy under the Constitution

---

91. *See id.* at 318.

92. *See* 5 U.S.C. § 552a(b).

93. *Id.* § 552a(b)(3). The Act defines "routine use" as "the use of [a] record for a purpose which is compatible with the purpose for which it was collected." *Id.* § 552a(a)(7).

94. *See* OTA, *supra* note 12, at 41 n.39. For examples, as well as a critical review, of agencies' broad interpretation of the routine use exemption, see Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 978-90 (1991).

95. *See* OTA, *supra* note 12, at 79.

96. Gellman, *supra* note 87, at 134.

97. While the Constitution does not explicitly confer a right to privacy, the Supreme Court has recognized an implied right that protects from government intrusion an individual's interest in both autonomous decisionmaking and "avoiding disclosure of personal matters." Whalen v. Roe, 429 U.S. 589, 598-600 (1977). The Court has relied on the former interest to protect individuals' decisions regarding, among other things, child rearing, *see* Pierce v. Society of Sisters, 268 U.S. 510, 534-45 (1925), procreation, *see* Skinner v. Oklahoma, 316 U.S. 535, 541 (1942), contraception, *see* Griswold v. Connecticut, 381 U.S. 479, 484 (1965), marriage, *see* Loving v. Virginia, 388 U.S. 1, 12 (1967), and abortion, *see* Roe v. Wade, 410 U.S. 113, 152-56 (1973). The parameters of the right to privacy, however, are not clear, *see* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) (noting that the "full measure of the constitutional protection of the right to privacy has not yet been delineated"), and commentators frequently debate its limits, *see* Gostin, *supra* note 12, at 495. For a brief discussion of the development of the right to privacy, see OTA, *supra* note 12, at 39-40. For a discussion of the right to informational privacy specifically, see Bruce W. Clark, Note, *The Constitutional Right to Confidentiality*, 51 GEO. WASH. L. REV. 133 (1982).

offers protection only from intrusions by the government.[98] Because most health-related data are maintained by non-governmental entities, constitutional remedies are not available to individuals whose privacy is breached by private data-holders.[99] Furthermore, even when the information in question is held by a government agency, an examination of applicable case law indicates that an individual's ability to seek recourse under a constitutional right to informational privacy is limited.[100]

The most well-known health information privacy case, *Whalen v. Roe*,[101] also marked the beginning of the Supreme Court's articulation of a right to privacy in personal information.[102] In *Whalen*, the Court addressed the constitutionality of a New York statute directing physicians to notify the state when certain drugs were prescribed and requiring the state to store this individually identifiable information for a number of years.[103] The Court stated that the right to privacy encompasses two interests, an interest in individual autonomy and an interest in "avoiding disclosure of personal matters."[104] Despite the existence of these interests, and despite a recognition of a threat to privacy posed by computer databanks, the Court held that the statute did not violate any protected right to privacy.[105] The Court thought particularly persuasive the physical, technological, and organizational safeguards implemented by the state to protect the prescription information, and stated that these measures indicated sufficient concern for protecting the right to privacy.[106] It also noted that the right to privacy in information is not absolute but is subject to countervailing public interests.[107] Consequently, the Court concluded that the disclosure of information to government officials charged with protecting a

98. *See* Schwartz, *supra* note 12, at 314-15.

99. *See id.*

100. *See infra* notes 101-26 and accompanying text.

101. 429 U.S. 589 (1977).

102. *See* Schwartz, *supra* note 12, at 315.

103. *See Whalen*, 429 U.S. at 591-95.

104. *Id.* at 599. One commentator has noted that the *Whalen* decision "does little to ensure that future courts will hold health officials to exacting constitutional standards to protect privacy." Gostin, *supra* note 12, at 496. For critical analyses of the *Whalen* decision, see Schwartz, *supra* note 12, at 315-17; Terri Finkbine Arnold, Note, *Let Technology Counteract Technology: Protecting the Medical Record in the Computer Age*, 15 HASTINGS COMM. & ENT. L.J. 455, 481-83, 489-90 (1993); Clark, *supra* note 97, at 133-38; Wendy Parmet, Note, *Public Health Protection and the Privacy of Medical Records*, 16 HARV. C.R.-C.L. L. REV. 265, 294-98 (1981).

105. *See Whalen*, 429 U.S. at 602-06.

106. *See id.* at 592-95, 605.

107. *See id.* at 602.

community's health does not necessarily constitute a violation of constitutional protections.[108]

Subsequent federal courts have also decided in favor of the public interest. In *United States v. Westinghouse Electric Corp.*,[109] the Court of Appeals for the Third Circuit held that demands for access to Westinghouse's employee medical records by the National Institute for Occupational Safety and Health ("NIOSH") did not violate the employees' constitutional right to privacy.[110] The court recognized that the constitutional right to privacy applied because the employee medical records fell within the *Whalen*-defined interest of avoiding disclosure by the government of personal information.[111] It noted, however, that "the right of an individual to control access to her or his medical history is not absolute" and that "public health or other public concerns may support access to facts an individual might otherwise choose to withhold."[112] Applying a seven-point balancing test,[113] the court held that the public interest advanced by NIOSH's investigation into working conditions at the Westinghouse plant justified the "minimal intrusion" into the privacy of the employees' medical information.[114]

Fifteen years later, the Third Circuit reached a similar result in *Doe v. Southeastern Pennsylvania Transportation Authority* ("SEPTA").[115] SEPTA, a self-insured public employer, learned of employee Doe's HIV-positive status when performing a cost-assessment review of records maintained by the administrator of its

108. *See id.* The Court drew an analogy to state laws requiring the reporting of "injuries caused by deadly weapons" and suspected incidents of child abuse. *Id.* at 602 n.29.

109. 638 F.2d 570 (3d Cir. 1980).

110. *See id.* at 580-81.

111. *See id.* at 577.

112. *Id.* at 578.

113. The *Westinghouse* Court enunciated seven factors to consider when undertaking this balancing process: (1) the kind of record the government wishes to obtain; (2) the kind of information this record does or might contain; (3) the harm that may occur if this information is subsequently disclosed without consent; (4) the injury that may occur to the relationship that produced the record because of this disclosure; (5) the adequacy of measures designed to prevent unauthorized subsequent disclosure; (6) the degree of need for obtaining the information; and (7) whether there exists a statutory mandate or other clear public interest favoring access to the information. *See id.*

114. *Id.* at 580. The court did hold that employees were entitled to prior notice of the disclosure. *See id.* at 580-81.

115. 72 F.3d 1133 (3d Cir. 1995). For further analysis of *SEPTA*, see Kari C. Kwiatkowski, *Extension of the Right to Privacy to Medical Prescription Information:* Doe v. Southeastern Pennsylvania Transportation Authority, 38 B.C. L. REV. 433 (1997).

employee prescription drug program.[116] Applying the *Westinghouse* balancing test, the court held that SEPTA had not violated Doe's constitutional right to privacy in his prescription drug records.[117] The court recognized a "strong public interest ... in [SEPTA]... containing its costs and expenses by permitting this sort of research" and reasoned that this interest outweighed the "minimal" intrusion into Doe's privacy.[118]

Aside from public interest concerns, the constitutional right to privacy in health information is likely circumscribed in an additional way. In *United States v. Miller*,[119] the Supreme Court held that an individual's right to privacy in his financial records did not apply to information held about that individual by a third party.[120] Although *Miller* has since been superseded by the Right to Financial Privacy Act of 1978,[121] some commentators believe a similar outcome would result if an analogous case involving health information came before the Court.[122] Such a decision would likely mean that patients would not have standing to contest the constitutional validity of efforts by the government to access health information held about them by hospitals, doctors, and other third parties.[123]

These decisions demonstrate that the constitutional right to privacy does not adequately address the full range of issues related to the privacy of health information.[124] Individuals cannot rely on constitutional rights to protect their privacy because the courts are likely to determine that countervailing public interests justify access to information by the government.[125] As long as this trend continues, legislation and administrative regulations will be more preferable mechanisms through which to create strong health privacy

116. *See SEPTA*, 72 F.3d at 1135-36.
117. *See id.* at 1140.
118. *Id.*
119. 425 U.S. 435 (1976).
120. *See id.* at 443.
121. *See supra* note 82 and accompanying text.
122. *See* H.R. REP. NO. 103-601, pt. 5, at 69 (1994) (expressing the Committee's belief that "there is a substantial risk that *Miller* would be applied to health records"); *see also* Gellman, *supra* note 20, at 290-91 (describing the likelihood of a similar outcome as "real" and noting that "[a]s a practical matter, in the absence of a statute or a definitive court decision, the *Miller* decision is effectively being applied when medical records are subpoenaed").
123. *See* Gellman, *supra* note 20, at 290-91.
124. *See* Gostin, *supra* note 12, at 498.
125. *See id.* at 497 ("Provided the government articulates a valid societal purpose and employs reasonable security measures, courts have not interfered with traditional governmental activities of information collection.").

protections.[126]

3. Health Information Privacy Protections at the State Level

The absence of meaningful federal statutes and the unwillingness or inability of federal courts to provide strong constitutional safeguards mean that the task of protecting health information has fallen on the states.[127] A majority of states provide some measure of confidentiality protection for health-related data through the common law.[128] For example, breach of fiduciary duty,[129] breach of implied contract,[130] invasion of privacy,[131] and breach of confidentiality[132] have served as causes of action for individuals seeking private redress for the nonconsensual, extrajudicial disclosure of health information. Largely by default, these causes of action probably provide the "most consistent safeguards" for the confidentiality of health information.[133]

The common law approach, however, is not without limitation. For instance, certain duties—notably a duty of confidentiality—normally apply only to those in a fiduciary relationship with the patient—usually doctors.[134] Insurers and most secondary users normally do not owe fiduciary duties to patients and, therefore, are not subject to these common law causes of action.[135] Unless the state

126. *See id.* *But see* Parmet, *supra* note 104, at 294 (arguing that the legislative approach is disfavored because "the legislature remains free to create numerous [statutory] exceptions" and that "[c]onstitutional doctrines must be utilized to attack the deficiencies of this legislative solution").

127. *See* Gostin, *supra* note 12, at 498.

128. *See id.* at 508.

129. *See, e.g.*, Horne v. Patton, 287 So. 2d 824, 829-30 (Ala. 1973).

130. *See, e.g.*, Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793, 801 (N.D. Ohio 1965).

131. *See, e.g.*, *Horne*, 287 So. 2d at 830-31. Two torts based on a right to privacy are particularly relevant—unreasonable intrusion of privacy and public disclosure of private facts. *See* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 854-59 (5th ed. 1984). To state a cause of action for the former, one must show intentional interference with one's interest in "solitude or seclusion." *Id.* at 854. Publication of the information obtained is not an element of the tort. *See, e.g.*, Rogers v. Loews L'Enfant Plaza Hotel, 526 F. Supp. 523, 528 (D.D.C. 1981) (citing Pearson v. Dodd, 410 F.2d 701, 704 (D.C. Cir. 1969)). The latter generally requires a showing of public disclosure of private facts that "would be highly offensive and objectionable to a reasonable person of ordinary sensibilities." KEETON ET AL., *supra*, at 856-57; *see also infra* note 139 (describing a possible limitation on the use of public disclosure of private facts as a cause of action).

132. *See, e.g.*, Humphers v. First Interstate Bank, 696 P.2d 527, 533-36 (Or. 1985) (en banc).

133. Gostin, *supra* note 12, at 510.

134. *See id.* at 510-11.

135. *See id.* at 510 (citing Hague v. Williams, 181 A.2d 345, 349 (N.J. 1962)).

has enacted such a duty by statute,[136] individuals frequently have no legal recourse against insurers, private businesses, and others who disseminate health information without consent.[137] This limitation is particularly significant because the redisclosure of information by secondary users is considered one of the principal threats to health information privacy.[138] Furthermore, several commentators have suggested that torts based on the right to privacy are strictly circumscribed and difficult to apply to situations involving the disclosure of health information.[139]

Each state has augmented its common law protections with statutes concerning the confidentiality of health information, but very few states have comprehensive statutory protections.[140] Like Congress, state legislatures have enacted privacy laws in piecemeal fashion.[141] The result of this ad hoc approach has been a proliferation of laws pertaining directly or indirectly to the confidentiality of health information. A 1979 survey of health information confidentiality laws found, for example, that the number of statutes ranged from seven in Vermont to thirty-nine in Hawaii.[142] The results of a 1996 survey of state confidentiality laws indicate that proliferation has continued unabated.[143]

---

136. Only a small minority of states have enacted confidentiality statutes that apply to entities unaffiliated with the delivery of care. *See infra* note 480 and accompanying text.

137. *See* Gostin, *supra* note 12, at 508-12.

138. *See supra* notes 37-50 and accompanying text.

139. The tort of disclosure of private facts has traditionally required a showing of public disclosure. *See* KEETON ET AL., *supra* note 131, at 856-57. To satisfy the public disclosure requirement, a plaintiff generally must show that the information about him was communicated to the public at large, not just to one person or several persons. *See, e.g.*, Santiesteban v. Goodyear Tire & Rubber Co., 306 F.2d 9, 11 (5th Cir. 1962) (construing Florida laws to require communication to the "public in general" or to a "large number of persons as distinguished from one individual or a few"); Vogel v. W.T. Grant Co., 327 A.2d 133, 137-38 (Pa. 1974) (holding that disclosure of one plaintiff's poor credit record to four persons did not satisfy the publication requirement for a disclosure of a private facts cause of action). Because many misuses of health data do not involve such widespread disclosure, this cause of action might be unavailable. *See* Gostin, *supra* note 12, at 509 n.291; Schwartz, *supra* note 12, at 321-22.

140. *See* Gostin, *supra* note 12, at 506. California enacted one of the most comprehensive health information confidentiality statutes in 1981. *See* CAL. CIV. CODE §§ 56.05-.37 (West 1982 & Supp. 1998).

141. *See, e.g.*, William J. Fenrich, Note, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 970 (1996) (citing Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 205, 208-09 (1992)).

142. *See* Gellman, *supra* note 87, at 136 n.33 (citing NATIONAL COMM'N ON CONFIDENTIALITY OF HEALTH RECORDS, HEALTH RECORDS CONFIDENTIALITY LAWS IN THE STATES 17-19, 54 (1979)).

143. *See* LAWRENCE O. GOSTIN ET AL., LEGISLATIVE SURVEY OF STATE

One significant finding of the 1996 survey is the degree to which statutory protections for health information can vary within a state. Because of state legislatures' piecemeal approach to privacy, different levels of confidentiality protection may apply depending on the kind of data involved and the identity of its custodian.[144] Many states have enacted, for example, disease-specific statutes addressing the use and dissemination of information related to mental illness, genetic testing, HIV infection, and other conditions deemed particularly sensitive.[145] These statutes typically confer a higher degree of confidentiality protection than other statutes pertaining to health information generally.[146]

The survey also reconfirmed that states differ greatly in the level of confidentiality protection they provide to health information. It found, for example, that every state has statutes that directly or indirectly concern HIV-related information, but that these statutes "vary considerably" in how stringently they protect the information.[147] Massachusetts law, for example, prohibits virtually without exception the disclosure of HIV test results without the written consent of the individual.[148] Statutes in New York and California, on the other hand, each list more than a dozen exceptions to their consent requirements.[149] The survey noted significant discrepancies among the states concerning other kinds of confidentiality statutes as well. Thirty-seven states impose a statutory duty of confidentiality on doctors, but only twenty-six impose this duty on other health care providers, and only nine extend it to institutions not affiliated with the delivery of care, such as employers.[150]

States that do impose a duty of confidentiality frequently require consent to disclose information concerning a patient.[151] These states differ, however, in their approach to the consent process. The survey found that California has detailed requirements concerning consent

---

CONFIDENTIALITY LAWS, WITH SPECIFIC EMPHASIS ON HIV AND IMMUNIZATION (REPORT TO THE U.S. CENTERS FOR DISEASE CONTROL ET AL.) (1996).

144. *See id.* at 40, 43.

145. *See id.* at 43.

146. *See id.* at 43, 156.

147. *Id.* at 65, 77.

148. *See* MASS. ANN. LAWS ch. 111, § 70F (Law. Co-op. 1995 & Supp. 1998); GOSTIN ET AL., *supra* note 143, at 78.

149. *See* CAL. CIV. CODE § 56.10 (West 1982 & Supp. 1998); N.Y. PUB. HEALTH LAW § 2782 (McKinney 1993 & Supp. 1998); GOSTIN ET AL., *supra* note 143, at 78, 80.

150. *See* GOSTIN ET AL., *supra* note 143, at 48-51.

151. *See id.* at 54-55.

forms,[152] while some states do not even require that consent be given in writing.[153] Statutorily defined exceptions to the consent requirement vary as well. Sixteen states permit the nonconsensual disclosure of personally identifiable information to epidemiologists and other researchers, for example, but only eighteen states provide for such disclosure to other health care providers.[154]

Consent arguably has little meaning if patients are unaware of the contents of the information they permit to be disclosed.[155] While some states confer on individuals the right to inspect and copy health information held about them, as of February 1998, twenty-two states did not.[156] Where a right of access exists, its scope varies, with some states guaranteeing the right to inspect both hospital and physician records and other states securing a right to inspect hospital records only.[157]

States also differ significantly in their approach to the increasing role of computerization in health care information systems. According to the 1996 survey, twenty-two states have statutes with provisions governing the confidentiality of data in computerized format.[158] Other states merely attempt to apply statutes written in an era of paper-based information systems to computerized data.[159] Aware of the privacy concerns raised by computerization, a few states have even enacted so-called "quill-pen" statutes, which require health information to be maintained in paper format only.[160]

The result of this boggling array of state confidentiality laws is, as one commentator put it, "a legal, political and practical mess"[161] that has been widely criticized.[162] Notably, individuals receive

152. *See* CAL. CIV. CODE § 56.11 (West 1982).

153. *See* GOSTIN ET AL., *supra* note 143, at 55.

154. *See id.* at 54.

155. *See* OTA, *supra* note 12, at 70; PRIVACY COMMISSION, *supra* note 19, at 289; SECRETARY OF HEALTH AND HUMAN SERVS., CONFIDENTIALITY OF INDIVIDUALLY-IDENTIFIABLE HEALTH INFORMATION: RECOMMENDATIONS OF THE SECRETARY OF HEALTH AND HUMAN SERVICES 34 (1997) [hereinafter HHS RECOMMENDATIONS] ("A patient's decision whether to disclose a record may depend on what the record says, and so access to the record is integral to making an informed choice to disclose information.").

156. *See Health Care Information Confidentiality: Hearing on S. 1368 Before the Senate Comm. on Labor and Human Resources*, 105th Cong. 8 (1998) [hereinafter *Hearing on S. 1368*] (statement of AHIMA).

157. *See id.*

158. *See* GOSTIN ET AL., *supra* note 143, at 51.

159. *See id.* at 57.

160. *See Hearings on H.R. 4077*, *supra* note 48, at 222.

161. Gellman, *supra* note 87, at 137.

162. *See, e.g.*, INSTITUTE OF MED., HEALTH DATA IN THE INFORMATION AGE 151-52 (Molla S. Donaldson & Kathleen N. Lohr eds., 1994) [hereinafter HEALTH DATA IN THE

inconsistent levels of confidentiality safeguards for their health information; the degree of confidentiality depends on the subject of the data, the identity of the data-holder, and the state in which the data are held.[163] The current system of state laws also fails to recognize fundamental changes that have occurred in the way care is delivered and the means by which information is managed. As the health care industry continues its process of integration, institutions and provider networks have grown in size.[164] With computers replacing paper as the means of managing information, providers and other entities in the industry have been able to expand their operations without regard to geography.[165] Institutions with multi-state operations are forced to comply with a unique set of laws for each state, creating substantial administrative and financial burdens.[166] Multiple legal standards apply as data flow across state lines even in a single electronic transaction,[167] and in the event of litigation concerning that transaction, users of data face substantial uncertainty as to which state has jurisdiction.[168] Attempting to comply with the inconsistent laws breeds confusion, increasing the risk that data will be disclosed in violation of some law.[169] Furthermore, most state confidentiality obligations apply to specific users of information, ignoring the reality of data sharing among many different entities.[170] The end result is that those who use and share information are uncertain of their legal obligations, and individuals are unsure of their legal rights as information passes from state to

---

INFORMATION AGE]; OTA, *supra* note 12, at 15; Gostin, *supra* note 12, at 516; Schwartz, *supra* note 12, at 310, 320; *see also infra* notes 182-85 and accompanying text (describing widespread support for a comprehensive federal health confidentiality law).

163. *See* GOSTIN ET AL., *supra* note 143, at 155-57.

164. *See supra* notes 25-30 and accompanying text.

165. *See* Gellman, *supra* note 87, at 138-39.

166. *See, e.g.*, Thompson Statement, *supra* note 54, at 4 (noting that Revco Drug Stores has had to develop a computer system that conforms to the separate confidentiality requirements of the 17 states in which it operates). *But see* Steven Kenny Hoge, Testimony on Behalf of the American Psychiatric Association Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 51 (Feb. 18, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Hoge Testimony] (arguing that the administrative and financial burdens are not unlike those experienced by any interstate business).

167. *See Hearings on S. 1360*, *supra* note 54, at 107 (statement of the Association for Electronic Health Care Transactions).

168. *See* HEALTH DATA IN THE INFORMATION AGE, *supra* note 162, at 151.

169. *See* GOSTIN ET AL., *supra* note 143, at 155-57.

170. *See id.* at 58, 157. For a description of the various entities that might handle identifiable patient data in a single electronic transaction between provider and payer, see *Hearings on S. 1360*, *supra* note 54, at 107 (statement of the Association for Electronic Health Care Transactions).

state and from user to user.

III. LAYING THE GROUNDWORK FOR THE CURRENT DEBATE

A. *A Uniform State Approach?*

It is widely acknowledged that the current system of federal and state laws neither adequately protects patients' privacy nor facilitates the delivery of high-quality, cost-efficient care.[171] As demonstrated in Part II, the continuing integration of the health care industry and the increasing reliance on electronic data transactions mean that these problems will continue. In a 1993 report to Congress, the Office of Technology Assessment warned that unless a new approach is taken, health confidentiality issues will increasingly be resolved in the legislatures and the courts of the individual states, which will only exacerbate the problems already presented by the system of fifty sets of laws.[172]

One alternative approach, recommended by the Privacy Protection Study Commission in 1977, would have the fifty states enact a uniform law for the confidentiality of health information.[173] In 1985, the National Conference of Commissioners on Uniform State Laws proposed model legislation for such a uniform law.[174] At this time, only two states, Montana and Washington, have adopted sections of the Uniform Health Care Information Act ("UHCIA").[175] Like existing state statutes, the UHCIA does not fully reflect the realities of the modern health care industry. Although the UHCIA applies to both paper- and computer-based information systems, its provisions apply only to providers in a relationship with the patient and not to other users of data such as claims processors and third-party payers.[176] Uniform legislation under consideration by the

171. *See, e.g.*, HEALTH DATA IN THE INFORMATION AGE, *supra* note 162, at 151-52; OTA, *supra* note 12, at 15; Schwartz, *supra* note 12, at 310, 320. *But see* Hoge Testimony, *supra* note 166, at 47-50 (arguing that while additional protections are needed for data maintained by secondary users, additional statutory restrictions on providers are unnecessary because the existence of breach of confidentiality claims already provides effective protection for patients' privacy).

172. *See* OTA, *supra* note 12, at 20.

173. *See* PRIVACY COMMISSION, *supra* note 19, at 293-94.

174. *See* UNIF. HEALTH-CARE INFORMATION ACT, 9 U.L.A. 475 (1988).

175. *See* MONT. CODE ANN. §§ 50-16-501 to -533 (1997); WASH. REV. CODE ANN. §§ 70.02.005 to -.904 (West 1992 & Supp. 1997).

176. *See* UNIF. HEALTH-CARE INFORMATION ACT §§ 2-101 to 7-102, 9 U.L.A. 485-514; *see also* Gellman, *supra* note 87, at 136 n.32 ("Having been proposed before the era of health maintenance organizations, ... health database organizations and computer networks, the uniform act is now out-of-date."). The UHCIA is quite explicit in its

National Association of Insurance Commissioners ("NAIC")[177] would, on the other hand, impose confidentiality requirements on insurers and entities authorized to assume risk, but not on providers and other users of health data.[178]

Even a comprehensive proposal cannot, however, overcome a uniform law's principal drawback: Assuming that all fifty legislatures could pass some form of model legislation in a timely manner, discrepancies in the protection and management of information would remain to the extent that states adopt only certain sections or alter the uniform law's recommendations.[179] The likelihood that all fifty legislatures would enact the proposed model legislation without some material change is doubtful.[180] The result would not satisfy the need for a high degree of uniformity in confidentiality requirements—a necessity for both the health care industry, which increasingly operates across state lines, and patients, whose sensitive health information deserves strong protection regardless of location.[181] For this reason, a uniform confidentiality law at the state level is not the most promising solution to an urgent problem.

B. The Call for Federal Action

The idea of a comprehensive federal law that provides strong confidentiality protection for health information and clear guidelines for its use has gained popularity in recent years.[182] As the

---

rejection of a comprehensive approach, noting that the relationship between non-provider and patient differs from that of the doctor-patient relationship and that Congress and the states are addressing the confidentiality of health data held by non-providers through specific statutes. *See* UNIF. HEALTH-CARE INFORMATION ACT § 1-101 cmt., 9 U.L.A. 480-81. According to the UHCIA, the latter argument "indicate[s] as an empirical matter that a health-care information statute should not cover . . . nonhealth-care providers." *Id.* at 481.

177. *See* NAIC, Health Information Privacy Model Act (Draft of July 2, 1998). If adopted by NAIC, the proposed draft will replace NAIC's current model health confidentiality law.

178. *See id.* § 3. The proposal would apply to "entit[ies] required to be licensed or authorized by the [state insurance] commissioner to assume risk, including but not limited to an insurer, a hospital, medical or health service corporation, a health maintenance organization, a provider sponsored organization, . . . [or] a self-insured group fund." *Id.* NAIC proposes that states enact additional confidentiality laws to cover data holders who fall outside the jurisdiction of insurance commissioners. *See id.* § 3(A) note.

179. *See* GOSTIN ET AL., *supra* note 143, at 161-62 ("Enactment of a Uniform Act requires legislative or public initiatives in each of the . . . fifty states. . . . Even after universal adoption, variability could persist if some states opt to impose stricter standards for privacy protection than those in the model statute.").

180. *See* HEALTH DATA IN THE INFORMATION AGE, *supra* note 162, at 182.

181. *See supra* notes 162-70 and accompanying text.

182. *See, e.g.*, OTA, *supra* note 12, at 44; Gostin, *supra* note 12, at 456, 527; Roger E.

inadequacies of the current system of state laws have become apparent, support for federal health information confidentiality legislation has increased. This support is broad-based, involving a diverse range of organizations with various interests, including privacy advocacy groups, information processing companies, doctors, and health plans.[183] These groups have found common ground in the need for a comprehensive federal statute because "no one benefit[s] from the existing diversity and inconsistency" in confidentiality laws.[184] Although support may not be universal, it has sufficiently advanced to the point that the need for a comprehensive federal statute is no longer seriously debated.[185]

The basic building blocks of a federal health confidentiality law are not in dispute.[186] In a 1973 report, the U.S. Department of Health, Education, and Welfare recommended five "fair information" principles that should form the basis of confidentiality guidelines for any kind of data: (1) no data system should be

---

Harris, Note, *The Need to Know Versus the Right to Know: Privacy of Patient Medical Data in an Information-Based Society*, 30 SUFFOLK U. L. REV. 1183, 1217 (1997). The constitutional basis for a federal law is rooted in the Commerce Clause. *See* H.R. REP. NO. 103-601, pt. 5, at 83 (1994) (citing findings enumerated in the Fair Health Information Practices Act, H.R. 4077, 103d Cong. (1994)); Gellman, *supra* note 87, at 139 ("Today, there are few, if any, participants in health care treatment or payment activities who do not operate in interstate commerce.").

183. This diversity is illustrated by the participants at a 1993 conference on health information issues who expressed support for federal legislation: CIGNA Health Care, IBM, the American Medical Association, Computer Professionals for Social Responsibility, and the U.S. Public Interest Research Group. *See Hearings on S. 1360*, *supra* note 54, at 63 (statement of the Center for Democracy and Technology).

184. Gellman, *supra* note 87, at 140.

185. *See, e.g.*, NATIONAL COMM. ON VITAL AND HEALTH STATISTICS, HEALTH PRIVACY AND CONFIDENTIALITY RECOMMENDATIONS 3 (1997) [hereinafter NCVHS RECOMMENDATIONS] ("The Committee's hearings showed strong and widespread support for federal health privacy legislation."); Gellman, *supra* note 87, at 139 ("With only limited exceptions, there is a broad consensus that favors replacing state privacy laws with a uniform federal law."). It has been suggested that support among privacy advocates for a federal solution may have waned somewhat in recent years. *See* Gellman, *supra* note 87, at 140 n.47. However, the enactment of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), *see infra* notes 232-36 and accompanying text, has likely arrested any decline in support. Concern that the adoption of federal standards for the electronic exchange of information and the creation of a national patient identifier number will further erode privacy, *see infra* notes 233-35 and accompanying text, has led advocacy groups to argue that strong privacy protections are more necessary than ever, *see, e.g.*, American Psychiatric Association, APA President Herbert S. Sacks, M.D. Calls Administration Medical Confidentiality Bill "A Giant Leap Backward" 2 (Sept. 11, 1997) (press release) (on file with the *North Carolina Law Review*) (stating that the passage of HIPAA "make[s] it all the more important to enact meaningful medical records privacy legislation").

186. *See* OTA, *supra* note 12, at 18.

maintained in secret; (2) individuals should have means of determining what information is held about them and how it is used; (3) individuals should have means to amend incorrect information concerning themselves; (4) personal information should not be used for purposes other than those for which it was collected without the consent of the subject of the information; and (5) organizations that create, maintain, or disclose identifiable information must assure its reliability and take reasonable precautions to prevent its misuse.[187] These principles have served as the foundation of almost every effort to pass confidentiality legislation.[188]

What remains the subject of serious disagreement is how to translate these principles into practice.[189] While both privacy advocates and health industry organizations agree that a federal health confidentiality law is desirable, they do so with different objectives in mind.[190] Patient rights organizations and privacy advocates seek legislation rooted in the principle Professor Alan Westin calls "privacy," which he defines as "the question of what personal information should be collected or stored *at all* for a given social function" and what amount of control the individual will have over his personal information.[191] Advocates view federal legislation principally as a means of providing strong, baseline privacy protection for health information regardless of its location.[192] As such, they emphasize the need to minimize access to personal information to the extent possible and stress the importance of informed consent requirements.[193] While recognizing that society

187. SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., U.S. DEP'T OF HEALTH, EDUC., AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 41 (1973). The Department of Health, Education, and Welfare is now the Department of Health and Human Services.

188. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 7-8, 10; OTA, *supra* note 12, at 18.

189. *See infra* Part IV.

190. *See* Gellman, *supra* note 87, at 140.

191. ALAN F. WESTIN, COMPUTERS, HEALTH RECORDS, AND CITIZEN RIGHTS 6 (1976) (emphasis added).

192. *See, e.g., Hearings on S. 1360*, *supra* note 54, at 100-01 (statement of the ACLU).

193. *See Hearings on H.R. 52*, *supra* note 27, at 132 (statement of the American Psychiatric Association) (arguing that "[f]ederal legislation should not permit the disclosure of confidential information ... without the individual's consent except in narrowly-defined emergency circumstances"); Denise M. Nagel, Prepared Statement on Behalf of the National Coalition for Patient Rights et al. Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 2 (Feb. 19, 1997) (unpublished statement, on file with the *North Carolina Law Review*) [hereinafter Nagel Statement] (arguing that the right to privacy should be overcome only by a showing of "compelling public need" such as "dangerousness to self or others" or "epidemic control"); ACLU, ACLU Says New Medical Privacy Legislation Falls Short 1 (May 19,

sometimes requires access to personal information, privacy advocates critically question the need to circulate health information beyond the health care provider and regard the development of a health information infrastructure as a threat to the individual's ability to control the distribution of information about himself.[194]

By contrast, many users of health data seek legislation based on the principle Professor Westin calls "confidentiality," meaning "the question of how personal data collected for approved social purposes shall be held and used by the organization that originally collected it, what other secondary or further uses may be made of it, and when consent by the individual will be required for such uses."[195] Hospitals, insurers, information processing companies, managed care organizations, utilization review agents, health researchers, and others begin with the premise that access to and sharing of data are critical for a well-functioning health care system and necessary to achieve social goods such as the elimination of health care fraud and surveillance of emerging diseases.[196] They advocate the creation of a federal law that will remove the present obstacles to the flow of information and will provide clear and uniform rules concerning its use, storage, and transfer in a computerized environment.[197] While acknowledging the importance of privacy rights, these users of information believe that overly stringent guidelines will inhibit their ability to function and will rob society of the benefits they seek to provide.[198]

1998) (press release) (on file with the *North Carolina Law Review*) (stating the ACLU's belief that no disclosure of any kind should be allowed without written patient authorization).

194. *See, e.g.*, A.G. Breitenstein & Denise M. Nagel, Editorial, *Keep Your Health History Private*, L.A. TIMES, Aug. 20, 1997, at B7.

195. WESTIN, *supra* note 191, at 6. There are no universally accepted definitions for "privacy" or "confidentiality." *See* OTA, *supra* note 12, at 8. Legal scholars disagree on whether the terms represent the same, distinct, or overlapping ideas. *See id.* It is not the intention of this Comment to enter this debate; however, Professor Westin's treatment of these concepts supplies a useful framework for understanding an important distinction in how many in the health care industry and privacy community view the direction that comprehensive federal legislation should take.

196. *See infra* Part IV.C.1-5.

197. *See, e.g.*, Jeanne Schulte Scott, Prepared Statement on Behalf of the Association for Electronic Health Care Transactions Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 1 (Feb. 3, 1997) (unpublished statement, on file with the *North Carolina Law Review*) ("Many of the proposals that have been put forth ... are expected to give our industry clear guidelines.").

198. *See, e.g., Hearings on H.R. 52, supra* note 27, at 179 (statement of the American Hospital Association) (advocating a balance between protection of privacy and "the necessary flow of health information for clinical and administrative purposes");

Implicit in these positions is a long-standing tension between the right to privacy and the need for access to information about an individual's health.[199] Resolving this tension in a manner that a majority of interested parties will support is not an easy task. In a recent report to the Secretary of HHS, the National Committee on Vital & Health Statistics ("NCVHS") acknowledged that "[h]ealth privacy legislation presents only hard choices and difficult tradeoffs."[200] As one commentator has framed the dilemma, do we restrict access to health data so as to achieve "reasonable levels" of privacy, recognizing that many social needs will be negatively affected, or do we conclude that these social needs are so important that we are willing to forego a promise of "absolute or even significant" privacy in our health information?[201]

The weight of authority suggests that the latter choice is preferable to the extent that it acknowledges that privacy rights are not absolute; society has a legitimate need to access personally identifiable health information for certain purposes, and individuals cannot realistically expect to withhold all information about themselves at the expense of the public interest.[202] As a condition of

---

Thompson Statement, *supra* note 54, at 3 ("We do not support federal legislation that would needlessly interfere with communications between pharmacists and their patients and pharmacists and other health care providers.").

199. *See* Gostin, *supra* note 12, at 453, 513-16.

200. NCVHS RECOMMENDATIONS, *supra* note 185, at 3.

201. Gostin, *supra* note 12, at 455.

202. *See, e.g., Privacy in the Electronic Age*, *supra* note 75, at 23 (Prepared Statement of Donna Shalala, Secretary of HHS) ("Just like our free speech rights, privacy rights can never be absolute."); NCVHS RECOMMENDATIONS, *supra* note 185, at 3 ("[N]o one can expect that the health care system will be restructured solely in the interests of privacy and without regard to cost."); Gostin, *supra* note 12, at 515 (asserting that ethical claims in support of a health information infrastructure are as strong as ethical arguments in favor of privacy); Schwartz, *supra* note 12, at 309 ("Rather than creating an absolute individual power over personal information, the law should evaluate competing values and strike a balance between individual and societal interests. An individual's control over medical . . . information cannot be complete because, at least to some extent, these data reflect an outside social reality."). The House Committee on Government Operations echoed this view when favorably reporting (later unsuccessful) health privacy legislation during the health care reform debate of 1994. The Committee specifically noted that the legislation at hand was a "code of fair information practices bill" and not a "privacy bill." H.R. REP. NO. 103-601, pt. 5, at 82 (1994). The reason for this distinction, the Committee asserted, was that "[i]n the last decade of the twentieth century, it is simply not possible to propose legislation that can promise that health information will be absolutely private." *Id.* at 83. This viewpoint is not, of course, without its critics. For a contrary argument, see *Privacy in the Electronic Age Hearings*, *supra* note 75, at 108 (prepared statement of A.G. Breitenstein) ("[Proposals permitting non-consensual disclosures of information are] justified on the radical and dubious notion that American patients must give up their right to privacy in order to fulfill their 'public responsibility' to

access, however, users of information should abide by strong guidelines governing how they obtain personal information, to what purposes it may be put, and to whom it may be disclosed, and the interest of individuals in information concerning themselves must be recognized.[203] The "fair information" principles outlined above are widely considered the most promising means to "promote an individual's capacity for decisionmaking while also safeguarding society's interest in increasing the efficiency and quality of health service."[204]

C. *Failed Attempts to Enact a Federal Law*

Despite widespread agreement with the fair information principles, repeated attempts to enact a federal health confidentiality law have been unsuccessful. Since the development of the fair information practices code, there have been three major legislative efforts to pass confidentiality legislation.[205] Spurred by the 1977 report of the Privacy Protection Study Commission, numerous bills relating to health information privacy were introduced during the 96th Congress (1979-80).[206] One of the primary reasons that these bills failed was strong opposition by members of the health care industry.[207] Because the bills were introduced before the era of integration, interstate operations, and reliance on computerized networks, the industry did not then see any benefit in the creation of uniform privacy guidelines at the federal level and instead preferred to operate under existing state laws.[208] An additional reason for the failure of the bills was pressure from the law enforcement community

---

an increasingly complex health care system. This notion is historically foreign to the American democratic system.").

203. *See, e.g.*, Gostin, *supra* note 12, at 515-16 ("[O]ne of the burdens of achieving cost effective and accessible care is a loss of privacy. In exchange for this diminution in individual rights, the government is obliged to create reasonably strong assurances of fair informational practices, without losing the benefits of a health information system.").

204. Schwartz, *supra* note 12, at 309.

205. *See infra* notes 206-31 and accompanying text.

206. *See* S. 2330, 96th Cong. (1980); S. 865, 96th Cong. (1979); S. 503, 96th Cong. (1979); H.R. 3444, 96th Cong. (1979); H.R. 2979, 96th Cong. (1979); H.R. 2465, 96th Cong. (1979); H.R. 2115, 96th Cong. (1979); H.R. 361, 96th Cong. (1979); H.R. 360, 96th Cong. (1979).

207. *See* Gellman, *supra* note 87, at 139 (citing *Privacy of Medical Records: Hearings on H.R. 2979 and H.R. 3444 Before a Subcomm. of the House Comm. on Gov't Operations*, 96th Cong. 1088 (1979) (statement of the American Hospital Association)).

208. *See id.* As noted previously, the industry has made a dramatic turnaround in its position, solidifying the widespread political support needed for passage of a uniform federal law. *See supra* notes 196-98 and accompanying text.

not to enact restrictions on its access to health information.[209]

The bills of the 96th Congress were nonetheless significant for creating the legislative framework used in most subsequent efforts to create a comprehensive federal law. The bills embodied many of the fair information practice principles described previously.[210] For example, one of the most comprehensive pieces of legislation outlined procedures for patients to inspect and amend medical information held about themselves; required health institutions affected by the legislation to create written notices of the information practices; prohibited the disclosure of personally identifiable information without consent of the individual or statutory authorization; authorized nonconsensual disclosures for specific purposes only, including public health investigations, health research, and law enforcement; specified procedures, including warrant and subpoena requirements, for government agencies and law enforcement to obtain data; and required affected health institutions to keep an accounting of certain disclosures.[211] Essentially all of the health privacy legislation introduced since that time has incorporated these provisions with varying degrees of fidelity.[212]

Following the failure of these early bills, the movement to enact a comprehensive privacy law lay relatively dormant until the Clinton Administration's health care reform efforts of 1994. Representative Gary Condit[213] introduced one of the major pieces of health privacy legislation in the 103d Congress, the Fair Health Information Practices Act,[214] which was later incorporated into the Administration's health care reform legislation.[215] Although the Condit proposal failed along with the larger reform effort, it is notable for defining the scope of protected health information

209. *See Hearings on S. 1360*, *supra* note 54, at 63 (statement of the Center for Democracy and Technology); *see also infra* notes 415-17 and accompanying text (discussing why law enforcement desires access to health records).

210. *See supra* notes 186-88 and accompanying text.

211. *See* Federal Privacy of Medical Information Act, H.R. 5935, 96th Cong. (1979). For further analysis of H.R. 5935, see H.R. REP. NO. 96-832, pt. 1 (1980) (House Comm. on Gov't Operations).

212. *See infra* Part IV.

213. Representative Condit is a Democrat from California.

214. H.R. 4077, 103d Cong. (1994). A similar piece of legislation, the Health Care Privacy Protection Act, was introduced in the Senate by Senator Patrick Leahy, a Democrat from Vermont. *See* S. 2129, 103d Cong. (1994). This bill did not reach the floor.

215. *See* H.R. REP. NO. 103-601, pt. 5, at 67 (1994) (accompanying the Health Security Act of 1994, H.R. 3600, 103d Cong. (1994)).

broadly[216] and for introducing the concept of the "health information trustee." The bill defined a trustee as one who "creates or receives protected health information" while acting in the capacity of a health care provider, benefit plan, oversight agency, researcher, or public health agency or for judicial, administrative, legal, or law enforcement purposes.[217] Anyone meeting this definition who received personally identifiable information from another source would qualify as a trustee and would be subject to the Act's provisions,[218] thus ensuring that data would remain subject to confidentiality rules as it traveled from user to user. This approach addresses some of the problems posed by the current system of protection, in which state confidentiality laws frequently apply only to specific data users,[219] and most subsequent legislative proposals have incorporated the notion of the health information trustee for this reason.[220]

With the failure of President Clinton's reform efforts, the 104th Congress turned its attention toward more incremental changes. The Condit bill resurrected interest in a comprehensive federal law and several legislative proposals were forthcoming. In the House, Representative Jim McDermott[221] introduced the Medical Privacy in the Age of New Technologies Act.[222] The McDermott bill, although similar to the Condit bill in format, incorporated significantly more rigorous privacy protections than previous proposals.[223] In the

216. The bill defined "protected health information" as "any information, whether oral or recorded in any form or medium, that ... relates to the past, present, or future physical or mental health of an individual, the provision of health care to an individual, or payment for the provision of health care"; identifies the individual or reasonably could be used to identify the individual; and is created or received by a health provider, benefit plan, oversight agency, researcher, or public health agency. H.R. 4077 § 3(a)(3).

217. *Id.* § 3(b)(3), (6), (8), (9).

218. *See id.* §§ 3(b)(3), 101, 102(a), 103(a).

219. *See supra* note 144 and accompanying text.

220. *See, e.g.*, H.R. 1815, 105th Cong. § 3(7) (1997).

221. Representative McDermott, a Democrat from the state of Washington, is also a psychiatrist.

222. H.R. 3482, 104th Cong. (1996). Representative Condit also introduced a bill substantially similar to this proposal in the previous Congress. *See* H.R. 435, 104th Cong. (1996).

223. For example, unlike other proposals, H.R. 3482 would have required the consent of the individual for all disclosures of personally identifiable information to health researchers, *see* H.R. 3482 § 210(a); prohibited the matching, linking, or aggregating of any protected health information held by two or more health information trustees without specific authorization of the individual, *see id.* § 201(i); required a "specific nexus" between the need to identify an individual and a risk of death or injury to another for nonconsensual disclosure to public health agencies, *id.* § 209(a); and required health information trustees to follow specified additional privacy guidelines if requested by an

Senate, the Medical Records Confidentiality Act,[224] introduced by Senator Robert Bennett,[225] took a more permissive approach with provisions aimed at facilitating the flow of health information.[226] Although pleased with the general direction of the Bennett bill, much of the health care industry was dissatisfied with particular provisions and proposed changes that would allow them to support the bill fully.[227] By contrast, many privacy advocates viewed sections of the Bennett bill as a significant threat to privacy and sought numerous alterations to ensure more stringent regulation of the access, use, and disclosure of data.[228] While some of the changes sought by industry and privacy advocates were incorporated into a rewrite of the bill,[229]

---

individual, *see id.* § 201(c).

224. S. 1360, 104th Cong. (1995). Although there are no agreed upon definitions for "privacy" and "confidentiality," *see supra* note 195, under Professor Westin's definition, it is interesting to note that Representative McDermott introduced a "Privacy" bill while Senator Bennett introduced a "Confidentiality" bill.

225. Senator Bennett is a Republican from Utah. The bill garnered an impressive list of 20 co-sponsors, including Senators Thomas Daschle, Robert Dole, Orrin Hatch, Nancy Kassebaum, Edward Kennedy, and Patrick Leahy, and was often referred to as the "Bennett-Leahy" bill.

226. Compared with the McDermott bill, *see supra* notes 222-23, as introduced S. 1360 did not require the consent of the individual for the disclosure of information to health researchers, *see* S.1360 § 209(a), nor did it prohibit the linking of data held by two or more health information trustees, impose any relationship requirement between the identity of an individual and a specific threat to the public for nonconsensual disclosure to public health authorities, *see id.* § 208, or give individuals the right to request segregation of their health information and additional safeguards.

227. The health care industry was greatly concerned that the Bennett bill would place significant burdens on the use of intermediary agents, such as electronic claims processors, to transmit and store data. *See, e.g., Hearings on S. 1360, supra* note 54, at 109-11 (statement of the Association for Electronic Health Care Transactions) ("As introduced, this bill would wipe out the entire health information service industry."). The bill would have applied the responsibilities of trusteeship to these "health information services." S. 1360 § 3(6), (7)(A)(i). In theory, these agents would have had to obtain the consent of the patient to transmit the data to its ultimate, intended recipient and would also have been subject to demands by individuals to inspect their health information. *See id.* §§ 101-102, 202-203. Members of the health care industry were also concerned about how the bill's consent-to-disclose requirement would affect the circulation of information within an institution. *See, e.g., Hearings on S. 1360, supra* note 54, at 146 (statement of Health Industry Manufacturer's Association).

228. Changes sought by some public interest groups included refining the preemption section of the bill to permit states to enact more stringent privacy laws in a broad range of areas, *see, e.g., Hearings on S. 1360, supra* note 54, at 141-42 (statement of the Consumer Project on Technology), as well as restricting the nonconsensual access to information by health researchers, oversight agencies, public health agencies, and law enforcement, *see id.* at 145.

229. A revised but never formally introduced version of the bill was circulated in April of 1996. Among the changes reflected in the revised version were the addition of a section of principles underlying the bill, a new requirement that consent be obtained in most cases for the release of personally identifiable health data for use in health research,

neither side was completely satisfied and discussions became mired in disagreement.[230] The Bennett bill ultimately died due to lack of support from both industry and privacy advocates,[231] and the McDermott and reintroduced Condit bills saw little progress in a Republican-controlled House.

Although efforts to enact a comprehensive confidentiality law had once again failed, the 104th Congress did pass landmark health reform legislation with important provisions related to privacy. To facilitate the development of a health information infrastructure, the "Administrative Simplification" subtitle of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[232] requires the Secretary of HHS to adopt uniform standards for the electronic

---

and a new requirement that law enforcement meet a "clear and convincing" evidence standard for a warrant to obtain health-related information. *See* CDT POLICY POST (Ctr. for Democracy and Tech., Washington, D.C.), Apr. 12, 1996, at 1-2 <http://www.cdt.org/publications/pp_2.14.html>.

230. An informal "working group" was formed in an effort to reach a compromise agreeable to most interested parties. Participants in this working group included the AIDS Action Council, American Civil Liberties Union, American Health Information Management Association, American Hospital Association, American Medical Association, American Psychiatric Association, Association for Electronic Health Care Transactions, Center for Democracy and Technology, Center for Medical Consumers/New York Public Interest Group, Consumer Project on Technology, International Billing Association, JRI Health Law Institute, National Coalition for Patient Rights, *Privacy Journal*, Public Citizen's Health Research Group, and the U.S. Department of Health and Human Services. This diverse group of organizations was strongly divided on many aspects of S. 1360. *See* Memorandum from Chai Feldblum, Federal Legislation Clinic of Georgetown University Law Center, & Janlori Goldman, Center for Democracy and Technology, to Working Group on S. 1360 (Dec. 19, 1995) (on file with the *North Carolina Law Review*).

231. *See* Lee Siegel, *Bennett to Reintroduce Records Bill*, SALT LAKE TRIB., Nov. 14, 1997, at A1; *cf. Fraud, Abuse and Confidentiality*, APA FED. NEWSL. (Am. Psychiatric Ass'n), June-July 1996, at 4-6 <http://www.psych.org/pub_pol_adv/fn_jj96.html> (describing efforts by some privacy advocates to defeat the Bennett bill). One notable exception was the Center for Democracy and Technology ("CDT"), a "non-profit public interest organization ... [whose] mission is to develop ... public policies that advance democratic values and constitutional civil liberties in new computer and communications technologies." CDT POLICY POST, *supra* note 229, at 3. CDT believed the revised version of the bill to be "extremely strong" and urged the Senate Committee on Labor and Human Resources to approve it "unanimously." *Id.* at 1.

232. 42 U.S.C.A. § 1320d to d-8 (West Supp. 1998). HIPAA is commonly called "Kassebaum-Kennedy" in reference to the two senators most closely associated with the legislation. *See Health Insurance Portability and Accountability Act: Hearing on P.L. 104-191 Before the Senate Comm. on Labor and Human Resources*, 105th Cong. 1 (1997) (statement of Sen. Jeffords). For a detailed analysis of the Administrative Simplification provisions of HIPAA, see Françoise Gilbert, *Privacy of Medical Records? The Health Insurance Portability and Accountability Act of 1996 Creates a Framework for the Establishment of Security Standards and the Protection of Individually Identifiable Health Information*, 73 N.D. L. REV. 93 (1997).

exchange of health information and for the creation of a unique identification number for every person, provider, health plan, and employer.[233] Concurrent with these provisions, the Act also requires the Secretary to submit to Congress within twelve months "detailed recommendations on standards with respect to the privacy of individually-identifiable health information."[234] If Congress fails to pass legislation governing privacy standards for health data maintained in electronic format within thirty-six months of HIPAA's enactment, the Secretary is ordered to promulgate regulations that

233. *See* 42 U.S.C.A. § 1320d-2(a), (b) (West Supp. 1998). The Act also requires the Secretary to promulgate security standards for the protection of health information, *see id.* § 1320d-2(d)(1), and requires those who use health information to maintain "reasonable and appropriate administrative, technical, and physical safeguards," *id.* § 1320d-2(d)(2).

Privacy advocates, doctors, and the psychiatry community have strongly criticized portions of the Administrative Simplification subtitle of HIPAA as a threat to privacy. These groups especially oppose the requirement that the Secretary of HHS adopt standards for a unique patient identifier for each individual, fearing that increased ease of computerized access will facilitate the abuse of confidential health information, allowing a user of health information to track an individual's medical history. *See, e.g.*, American Psychiatric Association, *supra* note 185, at 1-2 (expressing doubt that HHS can develop a unique patient identifier system that will protect confidentiality); Breitenstein & Nagel, *supra* note 194, at B7 (calling the unique patient identifier provision a "ticking time bomb"); *Health Data: Implementation of Unique Patient Identifier May Be Cause for Concern About Abuse*, Health Care Daily Rep. (BNA) (July 24, 1998), *available in* WESTLAW, BNA-HCD database (describing AMA's opposition to implementation of a unique patient identifier until further research demonstrates its necessity). At the least, privacy advocates argue, HHS should not proceed with implementation of a unique patient identifier until a confidentiality law has been enacted. *See, e.g.*, *Hearings on H.R. 52*, *supra* note 27, at 54 (statement of Janlori Goldman, visiting scholar, Georgetown University Law Center).

Cognizant of the privacy concerns raised by the unique patient identifier, the Clinton Administration announced in late July 1998 that it would accede to a delay and would not permit implementation of the identifier until confidentiality legislation is enacted. *See Privacy: No Patient Health Identifier Until Privacy Bill Passes, Gore Says*, Health Care Daily Rep. (BNA) (Aug. 3, 1998), *available in* WESTLAW, BNA-HCD database. Also concerned about threats to privacy posed by an identification number, Republican legislators have introduced legislation that would require Congress's approval of any patient identification system promulgated by HHS, *see Health Data: Proposed Rule on Security Standards for Health Information to Be Out Within Days*, Health Care Daily Rep. (BNA) (Aug. 6, 1998), *available in* WESTLAW, BNA-HCD database (noting a provision promoted by House Republicans); *Politics & Policy Health Care IDs: Senate Moves to Delay Debut*, American Health Line (APN) (Sept. 4, 1998), *available in* WESTLAW, APN-HE database (noting legislation introduced by Republican Senator Kay Bailey Hutchison of Texas), or would revise HIPAA to eliminate the patient identifier requirement altogether, *see* H.R. 4281, 105th Cong. § 2 (1998) (introduced by Rep. Ron Paul, a Republican from Texas).

234. 42 U.S.C.A. § 1320d-2, Historical and Statutory Notes (West Supp. 1998) (Recommendations with Respect to Privacy of Certain Health Information).

will create such standards.[235] HIPAA has, in effect, set a deadline for congressional action; if a federal health confidentiality law is not enacted by August 21, 1999, HHS regulations will determine, in part, the privacy rights of individuals and the responsibilities of data holders, an outcome both privacy advocates and the health care industry wish to avoid.[236]

Should Congress fail to act, it would not be the first deadline it has missed. On October 24, 1998, the European Union ("E.U.") data privacy directive ("Directive")[237] took effect, by which time the privacy laws of all E.U. member states were required to conform to its provisions.[238] The Directive generally requires data holders to inform data subjects of information held about them;[239] collect data only for specified and legitimate purposes; maintain the accuracy of the data; remove identifiers as soon as possible;[240] take steps to prevent the accidental destruction or loss of data or the unauthorized alteration or disclosure of data;[241] and, in certain circumstances, to obtain the data subject's consent for disclosure.[242] The Directive also grants data subjects the right to inspect data held about them and to object to certain uses of such data.[243] Of specific concern is a provision that prohibits the transfer of personally identifiable data between E.U. members and nations without data standards that ensure "an adequate level of protection."[244] While the Directive provides certain exceptions to this provision,[245] there is much concern that the failure of the United States to enact a health confidentiality law will interrupt the flow of health data between the United States

235. *See id.* (citing § 264(c)(1) of the HIPAA legislation, P.L. 104-191).

236. *See, e.g.*, NCVHS RECOMMENDATIONS, *supra* note 185, at 2 (noting that there is "virtually no industry or public support" for the regulatory approach but instead a "clear and strong preference for a legislative solution"). One reason for the preference for legislation is that HHS's regulatory powers under HIPAA would extend only to electronic health data. *See supra* notes 233-35 and accompanying text. It would be difficult to implement and enforce rules that apply to health information in electronic format but not to data in paper format. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 2. Another reason, of course, is that it would be more difficult to alter rights and obligations imposed by statute than for a government agency to promulgate new regulations.

237. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 32, 1995 O.J. (L 281) 31, 49.

238. *See id.*

239. *See id.* art. 10, at 41.

240. *See id.* art. 6, at 40.

241. *See id.* art. 17, at 43.

242. *See id.* art. 7, at 40.

243. *See id.* art. 12, at 42.

244. *Id.* art. 25, at 45-46.

245. *See id.* art. 26, at 46.

and Europe[246]—particularly personally identifiable data used for medical research and public health purposes.[247]

D. *Post-HIPAA Developments at the Federal Level*

Pursuant to HIPAA's requirements, HHS Secretary Donna Shalala presented the Clinton Administration's recommendations for health privacy legislation to Congress in September 1997.[248] Like previous legislative proposals, the recommendations incorporate the basic principles of fair information practices: patients should have the right to access, inspect, and petition to amend information about themselves; health information should not be disclosed to others without the consent of the individual or explicit statutory authorization; disclosure of information should be limited to the minimum amount necessary to accomplish the purpose of the disclosure; information should be used only for purposes compatible with and related to the purpose for which it was collected or received; and those who use health information must take reasonable steps to ensure its reliability and confidentiality.[249] In her congressional testimony, however, Secretary Shalala noted that these principles

246. *See, e.g., Hearing on S. 1368, supra* note 156, at 7 (opening statement of Sen. Jeffords). Although the present amount of identifiable health data exchanged between Europe and the United States is relatively small, the continued growth of electronic commerce will make such exchanges "commonplace" in the future. *Id.* at 131 (statement of the European Union).

247. Public health and research information comprise much of the international movement of individually identifiable health data. For instance, the U.S. Centers for Disease Control and Prevention imports health data from other countries as part of its public health investigations, while medical centers and pharmaceutical companies share clinical-trial data with counterparts around the world. *See* LOWRANCE, *supra* note 66, at 20.

248. *See Privacy in the Electronic Age Hearings, supra* note 75, at 3-7 (statement of Donna E. Shalala, Secretary of HHS). HIPAA required the Secretary to consult with the National Committee on Vital & Health Statistics ("NCVHS") in preparing recommendations for health privacy legislation. *See* 42 U.S.C.A. § 1320d-2, Historical and Statutory Notes (West Supp. 1998) (Recommendations with Respect to Privacy of Certain Health Information). Pursuant to this requirement, the NCVHS Subcommittee on Privacy and Confidentiality held eight days of public hearings involving more than 80 witnesses from a wide range of health care industry, public interest, state government, public health, and research organizations and agencies. *See* Letter from Don E. Detmer, M.D., Chairman, National Committee on Vital and Health Statistics, to Donna E. Shalala, Secretary of HHS 1 (June 27, 1997) (on file with the *North Carolina Law Review*). The Committee's report to the Secretary found that "[t]he United States is in the midst of a health privacy crisis" and recommended that the Clinton Administration "assign the highest priority to the development of a strong position on health privacy." NCVHS RECOMMENDATIONS, *supra* note 185, at 1-2. For discussion of the Committee's findings and recommendations on specific health privacy issues, see *infra* Part IV.

249. *See* HHS RECOMMENDATIONS, *supra* note 155, at 8-9.

must be weighed against the principle of "public responsibility" and that legislation must strike a balance between privacy and societal interests; health care information must be made available, she argued, for public health, antifraud, law enforcement, and other necessary purposes.[250]

Various provisions in the Administration's recommendations met with immediate criticism. Public interest groups and the psychiatric community have condemned the proposal as a threat to privacy for permitting, in their view, easy access to information by numerous parties, especially law enforcement.[251] At the same time, some members of the health care industry have expressed concern that certain recommendations, if enacted into law, would inhibit worthwhile activities such as health research.[252]

While HHS formulated its recommendations, the Administration addressed the confidentiality issue through other means. In September 1996, President Clinton issued an executive order creating the Advisory Commission on Consumer Protection and Quality in the Health Care Industry ("Commission").[253] At the President's behest, in November 1997 the Commission formulated a Patient Bill of Rights ("Bill of Rights") for health care.[254] The Commission articulated eight areas of consumer rights and responsibilities, including a right to privacy: "Consumers have the right to communicate with health care providers in confidence and to have the confidentiality of their individually identifiable health care information protected. Consumers also have the right to review and

250. *Privacy in the Electronic Age Hearings*, *supra* note 75, at 5-6 (testimony of Donna E. Shalala, Secretary of HHS).

251. *See, e.g.*, ACLU, Clinton Privacy Recommendations Open Medical Records to Desktop Snooping 1-2 (Sept. 11, 1997) (press release) (on file with the *North Carolina Law Review*); American Psychiatric Association, *supra* note 185, at 2.

252. *See, e.g.*, Lisa Seachrist, *Shalala's Medical Privacy Report Gets Mixed Reviews*, BIOWORLD Today, Sept. 15, 1997, at 3, *available in* 1997 WL 1130970 (reporting concern of the Pharmaceutical Manufacturers and Researchers of America that conferring on patients the right to demand inspection of their health information would frustrate clinical research trials). For discussion of privacy issues and research, see *infra* notes 326-59 and accompanying text.

253. *See* Exec. Order No. 13,017, 3 C.F.R. 215-16 (1997). The purpose of the Commission is to "advise the President on changes occurring in the health care system and recommend such measures as may be necessary to promote and assure health care quality and value, and protect consumers and workers in the health care system." *Id.* The Commission consists of 34 representatives from consumer organizations, health care providers, health plans, insurers, business, and government.

254. *See* ADVISORY COMM'N ON CONSUMER PROTECTION AND QUALITY IN THE HEALTH CARE INDUS., CONSUMER BILL OF RIGHTS AND RESPONSIBILITIES: REPORT TO THE PRESIDENT OF THE UNITED STATES (1997).

copy their own medical records and request amendments to their records."[255] Pursuant to this right, the Commission concluded: health information should not, except in limited circumstances, be used for non-health purposes without consent; when practicable, anonymized data should be used instead of individually identifiable data; non-consensual disclosures should be permitted only in limited circumstances; and, when disclosures must occur, only the minimum amount of information necessary to effect the purpose should be disclosed.[256] President Clinton endorsed the Commission's findings and urged the private sector to adopt voluntarily these and other provisions of the Bill of Rights.[257] The President also ordered federal agencies to review their health-related programs for compliance with the Bill of Rights and called on Congress to pass legislation as soon as possible that would make these rights "the law of the land."[258]

Separate from a Bill of Rights, several members of the 105th Congress have introduced their own stand-alone health

255. *Id.* at 53.

256. *See id.*

257. *See* President's Remarks Announcing the Health Care "Consumer Bill of Rights and Responsibilities," 33 WEEKLY COMP. PRES. DOC. 1868, 1870-71 (Nov. 24, 1997). The President noted that telecommunications giant GTE is the first large company to guarantee the provisions of the bill of rights to all persons covered by its health plan. *See id.* at 1871.

258. *Id.* at 1870-71. In February 1998, President Clinton issued a memorandum directing the Secretaries of Defense, Health and Human Services, Labor, and Veterans Affairs ("V.A.") and the Director of the Office of Personnel Management to ensure that their programs—including Medicare, Medicaid, the military health system, the V.A. health system, and the Federal Employees Health Benefits Plan—comply with the principles of the "Patient Bill of Rights," including the confidentiality provision. *See* Memorandum on Federal Agency Compliance with the Patient Bill of Rights, 34 WEEKLY COMP. PRES. DOC. 298, 298-99 (Feb. 23, 1998).

In the summer of 1998, Democractic members of Congress took up the President's challenge to enact a Patient Bill of Rights, *see* S. 1890, 105th Cong (1998); H.R. 3605, 105th Cong. (1998), and the Republicans responded with their own proposals, *see* S. 2330, 105th Cong. (1998); H.R. 4250, 105th Cong. (1998). All four bills included provisions relating to the confidentiality of health information, though none provided comprehensive protection. *See* S. 2330 §§ 211-232; S. 1890 § 122; H.R. 4250 §§ 5001-5004; H.R. 3605 § 122. The Republican-controlled House passed the Republican proposal, H.R. 4250, despite criticism from privacy advocates who argued that its confidentiality provisions would actually further erode patient privacy. *See Privacy: Confidentiality Language in House GOP Bill Draws Fire from Private Group*, Health Care Daily Rep. (BNA) (July 23, 1998), *available in* WESTLAW, BNA-HCD database. As of October 1998, the Senate had not acted on any Bill of Rights proposal; friction between the parties on the issue, coupled with a lack of time remaining in the current session, led some observers to predict that passage of any Bill of Rights legislation was unlikely. *See Insurance Regulation: Senate Returns to Continued Deadlock, New Uncertainty on Managed Care Reform*, Health Care Daily Rep. (BNA) (Aug. 31, 1998), *available in* WESTLAW, BNA-HCD database.

confidentiality bills. In January 1997, Representative Condit reintroduced his prior bill, now known as the Fair Health Information Practices Act of 1997.[259] Representative McDermott also reintroduced his confidentiality legislation, the Medical Privacy in the Age of New Technologies Act.[260] In the Senate, Senators Patrick Leahy and Ted Kennedy introduced the Medical Information Privacy and Security Act at the end of 1997,[261] while Senator Bennett circulated a draft of his proposed legislation.[262] Senator James Jeffords, Chairman of the Committee on Labor and Human Resources, intended to co-sponsor the Bennett proposal but withdrew his support because of policy disagreements with Senator Bennett.[263] Senator Jeffords subsequently introduced his own bill, the Health Care Personal Information Nondisclosure Act, in April

259. H.R. 52, 105th Cong. (1997). As introduced, H.R. 52 differs from its predecessor from the 104th Congress, H.R. 435, in several respects. Notably, H.R. 435 largely preempted state law, permitting states to enact more stringent rules only with regard to mental health and public health information. *See* H.R. 435, 104th Cong. § 304(a)-(b) (1995). H.R. 52 retains this provision but would also allow states to enact more stringent rules pertaining to the use and disclosure of information by state agencies. *See* H.R. 52 § 304(d); *Hearings on H.R. 52*, *supra* note 27, at 31 (statement of Rep. Gary Condit).

260. H.R. 1815, 105th Cong. (1997).

261. S. 1368, 105th Cong. (1997). The Leahy-Kennedy bill would force trustees to comply with requests by individuals to segregate specific information within their health records, prohibit the internal use or transfer of this segregated information without specific authorization by the individual, and prohibit the maintenance of this information in a computerized format. *See id.* § 202(f). It also would not preempt any state or federal law that provided for more stringent protections. *See id.* § 401(a). The Leahy-Kennedy bill differs substantially with the Condit bill in these areas, *see supra* note 259, but mirrors similar provisions in the McDermott bill permitting segregation of information, *see* H.R. 1815 § 201(c), and more stringent state laws, *see id.* § 402(a). For discussion of the desirability for differing confidentiality standards for different kinds of information, see *infra* notes 493-502 and accompanying text. For discussion of whether patients should be able to determine the medium of information storage, see *infra* notes 520-29 and accompanying text.

262. *See Privacy: House Republican Task Force Working on Legislation to Protect Patient Data*, Health Care Daily Rep. (BNA) (July 13, 1998) *available in* WESTLAW, BNA-HCD database.

263. Senator Jeffords grew concerned that Congress would not enact a health confidentiality law before the E.U. Directive took effect. *See Jeffords and Dodd Say Privacy Bill Must Help U.S. Companies Beat E.U. Data Deadline*, HEALTH LEGIS. & REG. WKLY., Apr. 8, 1998, *available in* 1998 WL 10395736. He apparently believed that Senator Bennett's most recent proposal, which would provide for complete preemption of state law, would not gain sufficient support among privacy advocates to pass. *Cf. id.* (reporting that Senator Jeffords's concern about the E.U. Directive deadline led him "to halt temporarily his attempt to find common ground" with Senator Bennett and instead introduce his own legislation that would permit more stringent state laws pertaining to mental health and public health data); *see also infra* note 514 and accompanying text (describing preemption provisions of Sen. Jeffords's bill).

1998.[264]

IV. SIGNFICANT ISSUES FOR HEALTH CONFIDENTIALITY LEGISLATION

HIPAA and the E.U. Directive have created a sense of urgency in the effort to enact a comprehensive federal law governing the rights and responsibilities of parties in relation to health information.[265] Because Congress failed to enact comprehensive legislation by the time the E.U. Directive took effect in October 1998, our ability to exchange health information with E.U. member states may already be restricted. And, if Congress fails to act by August 1999, regulations will determine the extent of protection covering computerized health data within the United States. Whether Congress will be able to enact any of the proposals currently before it remains to be seen. An inability to reach agreement on a number of issues in a way that satisfies most parties has been the principal stumbling block to the enactment of a federal law.[266] An analysis of recent efforts to enact a comprehensive federal law reveals that although there are numerous areas of agreement, significant differences of opinion remain.

A. What Is Protected Health Information?

There is widespread agreement that the scope of protected information in any federal law should be drawn as broadly as possible to reflect the vast amount of data collected today. In almost every proposal, "protected health information" is defined with such breadth as to encompass any individually identifiable information created or used by a health information trustee in the treatment or payment process.[267] Protected health information would, therefore, include: "traditional" treatment data such as diagnoses and medication history; other sensitive, personal information including Social Security numbers and financial information; and even information often considered "public," such as names, addresses, and

264. S. 1921, 105th Cong. (1998).

265. *See, e.g., Hearing on S. 1368*, *supra* note 156, at 7 (opening statement of Sen. Jeffords) (noting the deadlines set by HIPAA and the E.U. Directive and emphasizing that enacting a health confidentiality law is one of the committee's "highest priorities").

266. *See infra* note 530 and accompanying text.

267. *See, e.g.*, H.R. 1815, 105th Cong. § 3(16) (1997) (sponsored by Rep. McDermott); S. 1360, 105th Cong. § 3(14) (1995) (sponsored by Sen. Bennett); HHS RECOMMENDATIONS, *supra* note 155, at 20-21.

educational history.[268]

Anonymized information—data that do not directly identify an individual and for which there is no reasonable basis to believe that an individual can be so identified—poses little or no threat to personal privacy and would not fall under the purview of any currently proposed legislation.[269] For example, researchers who wish to conduct a study using health records already stripped of identifiers would not have to comply with statutory requirements concerning access to information for purposes of research. Because no strict guidelines exist for determining when information is and is not identifiable, present and past proposals have used only a test of reasonable likelihood.[270] It is clear that the results of applying this standard will vary depending on the identity of the user of information[271] and that, in some circumstances, the disclosure of seemingly generic information may establish the requisite likelihood.[272]

B. Right of Inspection and Amendment

There is broad consensus that individuals should have the right to access and request amendment of information held about themselves.[273] This consensus has relatively recent roots. Patients have traditionally been unable to access health information held

268. *See* OTA, *supra* note 12, at 80. It is irrelevant that some persons, including the individual who is the subject of the information, might not consider a particular piece of data to be sensitive. If the information is created or obtained in the process of treatment or payment by a party subject to the legislation and can be linked with an individual, it is protected health data. *See id.*

269. *See, e.g.*, H.R. 1815 § 3(16); HHS RECOMMENDATIONS, *supra* note 155, at 20-22.

270. *See, e.g.*, H.R. 1815 § 3(16); H.R. REP. NO. 103-601, pt. 5, at 87 (1994) (discussing the Fair Health Information Practices Part of the Health Security Act of 1994, H.R. 3600, 103d Cong. 1994)); HHS RECOMMENDATIONS, *supra* note 155, at 20.

271. For example, it is unreasonable to believe that the average recipient would be able to identify the subject of a record containing only a fingerprint; however, the same record would be protected health information if disclosed to law enforcement officers because they may have the ability to identify the individual. *See* H.R. REP. NO. 103-601, at 87.

272. For example, describing an individual as a famous "professional athlete" with "amyotrophic lateral sclerosis" could have provided a reasonable basis for identifying Lou Gehrig. *Id.*

273. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 7 ("The Committee found no disagreement with the basic principle of patient access and amendment rights."). For a discussion of patients' right to see their own medical records, as well as a proposed uniform law guaranteeing such a right, see Ellen Klugman, Comment, *Toward a Uniform Right to Medical Records: A Proposal for a Model Patient Access and Information Practices Statute*, 30 UCLA L. REV. 1349 (1983).

about themselves,[274] and even today only twenty-eight states guarantee a right of inspection.[275] The traditional justification offered for denying access is that physicians should have the ability to withhold information they believe may be detrimental to the patient's health.[276] This paternalistic reasoning conflicts, however, with the principle of self-determination.[277] Authority to disclose information about oneself is predicated on the doctrine of informed consent,[278] but consent is not truly informed if the person who is the subject of the information does not know its contents.[279] Some courts have also noted that patients possess a recognizable property interest in their health information that confers a right to inspect and copy the contents of their medical record.[280] Other justifications advanced for a right of inspection include educating patients about their health status, ensuring the accuracy of information contained within a record, and ensuring that the record supports charges for services rendered.[281]

For these reasons, inspection rights have been an integral principle of confidentiality legislation since the first statement of fair information privacy practices in 1973.[282] Health confidentiality bills generally include a provision conferring the right to inspect and copy information and, if the individual disagrees with its contents, to file a petition for amendment.[283] Only in narrow, statutorily defined circumstances can the data holder deny the request to inspect.[284] The data holder may refuse to grant a requested amendment but must

274. *See* OTA, *supra* note 12, at 71.

275. *See supra* notes 156-57 and accompanying text.

276. *See* OTA, *supra* note 12, at 71.

277. *See id.*

278. *See id.* at 70.

279. *See supra* note 155 and accompanying text.

280. *See, e.g.*, WESTIN, *supra* note 191, at 29 (citing cases upholding a right to inspect based on a patient's interest in her health information). Those who create a health record own the record itself, *see, e.g.*, JO ANNE CZECOWSKI BRUCE, PRIVACY AND CONFIDENTIALITY OF HEALTH CARE INFORMATION 12-13 (1984), but the individual is generally deemed the owner of the data contained within the record, *see id.* at 13; OTA, *supra* note 12, at 70; Gostin, *supra* note 12, at 522.

281. *See* OTA, *supra* note 12, at 72 (citing AMERICAN HEALTH INFO. MANAGEMENT ASS'N, POSITION STATEMENT 1 (1992)).

282. *See* SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., *supra* note 187, at 41.

283. *See* S. 1921, 105th Cong. §§ 101-102 (1998); S. 1368, 105th Cong. §§ 101(a), 102(a) (1997); H.R. 52, 105th Cong. §§ 101(a), 102(a) (1997); S. 1360, 104th Cong. §§ 101(a), 102(a) (1995). Medical records are not really "corrected," only amended. Information, even that which is discovered to be incorrect, is not stricken from a medical record. *See* BRUCE, *supra* note 280, at 123-24.

284. *See infra* notes 291-304 and accompanying text.

explain its reason for doing so.[285] The individual then has the right to file a letter explaining her position, which will accompany the disputed data on all subsequent disclosures.[286]

Although there is little debate concerning the existence of a right to inspect, some important differences in implementation remain. An issue of concern for the health care industry has been determining which data holders are required to permit inspections. At least one previous health confidentiality bill applied this requirement to all health information trustees regardless of function.[287] Some members of the health industry, notably electronic claims processors, have argued that the duty to permit inspection should not apply to parties who merely transmit or store data for others.[288] Because they have neither a direct relationship with the patient nor the medical expertise to judge amendment requests, these companies assert that it would be both improper and impractical to require them to permit access to data.[289] Acknowledging this argument, more recent proposals would generally exempt agents and contractors from the inspection and amendment obligations, thus requiring the patient to petition the person or entity that created the data, frequently the health care provider, which in turn can request the data from the agent.[290]

Another point of contention concerns statutory exceptions to the right to access.[291] An exception common to most proposals is the right to deny inspection if it is reasonably likely to endanger the life

285. *See, e.g.*, S. 1368 § 102(b); H.R. 1815, 105th Cong. § 102(b) (1997); S. 1360 § 102(b).

286. *See, e.g.*, S. 1368 § 102(c); H.R. 1815 § 102(c); S. 1360 § 102(c).

287. As introduced, the Medical Records Confidentiality Act of 1995 did not distinguish among data holders for purposes of the duty to permit inspection. *See* S. 1360 §§ 101-102.

288. *See, e.g.*, Robert B. Burleigh, Prepared Statement on Behalf of the International Billing Association Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 45-46 (Feb. 3, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Burleigh Statement].

289. *See Hearings on H.R. 52*, *supra* note 27, at 83-84 (prepared statement of Merida L. Johns, M.D., President of the American Health Information Management Association); Burleigh Statement, *supra* note 288, at 45-46. Doctors favor this approach as well, emphasizing that the health provider who generated the data should be the sole conduit for inspection requests. *See Hearings on H.R. 52*, *supra* note 27, at 60-61 (prepared statement of the American Medical Association).

290. *See, e.g.*, S. 1921, 105th Cong. §§ 101(g), 102(d) (1998); H.R. 3900, 105th Cong. §§ 201(g), 202(d) (1998); S. 1368 § 101(c); H.R. 1815 § 101(h)(1); H.R. 52, 105th Cong. § 101(g) (1997).

291. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 7-8.

or physical safety of any person.[292] The mental health community has advocated an additional exception that would allow the data holder to refuse access if he reasonably believes that harm will occur to the patient that outweighs the benefits of inspection.[293] Psychiatrists fear that a requirement to disclose to the patient the "understandings, interpretations, and thoughts of the practitioner" before the patient is ready will endanger the therapeutic process.[294] Although at least one proposal has incorporated this request,[295] others have not, perhaps because of a belief that a principal aim of a federal law is to empower the individual[296] or because of concern about what would be the proper standard for denial.[297]

Similarly, the pharmaceutical industry has argued that an exception should be created for certain kinds of research.[298] In "blinded" clinical drug trials, research subjects are not told the identity of the treatment they receive. For example, participants do not know if they are receiving the medication under study or a placebo.[299] A blanket right to inspect would allow participants to obtain this information and, the pharmaceutical community argues, raise questions about the scientific validity of the study.[300] The NCVHS found this argument persuasive but noted that no one could cite a single instance in which a demand to inspect information had negatively impacted a clinical drug trial.[301] The Clinton Administration, as well as Senator Jeffords, has nonetheless recommended a narrow exception for clinical trials,[302] but other

292. *See* S. 1921 § 101(b)(1); H.R. 1815 § 101(b)(1); H.R. 52 § 101(b)(2); S. 1360, 104th Cong. § 101(b)(1) (1995).

293. *See Hearings on S. 1360*, *supra* note 54, at 160 (statement of the American Psychiatric Association).

294. *Id.*

295. *See* S. 1921 § 101(b)(1) (permitting a refusal to allow inspection if the data holder reasonably believes that doing so could "cause substantial mental harm").

296. Representative Condit gave such an explanation for omitting the exception in his most recent bill, H.R. 52 § 101(b). *See Hearings on H.R. 52*, *supra* note 27, at 31 (statement of Rep. Gary Condit). He did note, however, that if a strong case could be made for the exception he would consider reinstating it. *See id.*

297. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 8.

298. *See* Richard S. Kent, Testimony on Behalf of the Pharmaceutical Research and Manufacturers of America Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 13 (Feb. 4, 1997) (unpublished transcript, on file with *North Carolina Law Review*).

299. *See id.*

300. *See id.*

301. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 8.

302. *See* S. 1921, 105th Cong. § 101(b)(4) (1998); HHS RECOMMENDATIONS, *supra* note 155, at 33. Under the Administration's proposal, for example, a trustee could deny the request for inspection by a clinical trial participant when "the information is collected

proposals have not followed suit.[303]

C. *Disclosure and Use of Protected Health Information*

There is unanimous agreement that data holders should generally obtain patient authorization before disclosing personally identifiable health data.[304] This principle, one of the five principles of fair information practices,[305] is based on the doctrine of informed consent; individuals have the same right to determine what happens to information about their bodies as they do to determine what happens to their bodies.[306] Consequently, proposals for a health confidentiality law generally begin with the basic requirement that data holders cannot disclose identifiable data, or use it for a purpose other than that for which it was collected, without the data subject's authorization.[307] Nonetheless, recognizing arguments that a consent requirement might unreasonably inhibit some legitimate demands for health information, most proposals also specify certain disclosures and uses of health data that would not require the patient's consent.[308] An analysis of some of the demands for health data reveals sharply divergent viewpoints on the proper number and breadth of exceptions to the consent requirement—as well as whether exceptions should be permitted at all.[309]

1. Disclosure for Treatment and Payment

Most proposals contain a requirement forbidding disclosure of identifiable health data for the purpose of providing care or payment for care without the patient's informed consent. Widespread concern exists, however, that there is a disjunction between the theory of informed consent and the reality of authorized disclosure in the modern health care system. With the advent of the third-party

---

in the course of a clinical trial, the trial is in progress, an institutional review board has approved the denial of access, and the patient has agreed to the denial of access when consenting to participate." HHS RECOMMENDATIONS, *supra* note 155, at 33.

303. *See, e.g.*, S. 1368, 105th Cong. § 101 (1997); H.R. 1815, 105th Cong. § 101(b) (1997); S. 1360, 104th Cong. § 101(b) (1995).

304. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 8.

305. *See supra* note 187 and accompanying text.

306. *See* OTA, *supra* note 12, at 70.

307. *See, e.g.*, S. 1921 §§ 201-203. Representative Shays's bill takes a different approach; H.R. 3900 expressly defines impermissible uses of health information, thus permitting other uses. *See* H.R. 3900, 105th Cong. § 101 (1998).

308. *See infra* notes 310-459 and accompanying text.

309. *See infra* notes 310-459 and accompanying text. The ACLU, for example, argues strenuously that a health confidentiality law should not permit any exceptions to the informed consent requirement. *See, e.g.*, ACLU, *supra* note 193, at 1.

payment system, many observers argue that an authorization-to-disclose requirement is meaningless in the case of payment for care because the patient has no real choice but to consent so that the provider may be paid.[310] This argument posits that consent to disclose is not truly informed because it fails the requirement of voluntariness.[311] There is also widely held concern that many authorizations fail the requirements of adequate disclosure and comprehension as well. Blanket and often vague disclosure authorization forms are presented to and signed by patients with such frequency that some observers question whether patients fully realize the consequences of their consent.[312]

Recognizing these concerns, the Clinton Administration's recommendations depart from the traditional approach to authorization rules taken by other legislative proposals. Rather than require the patient's authorization for the disclosure of information for health care treatment and payment purposes,[313] the Administration's plan would permit these disclosures by statute.[314] Arguably, this approach could actually raise awareness among patients about threats to confidentiality; because authorization would still be required for purposes other than health care treatment or payment, any request for authorization would alert the patient that the provider wishes to disclose information for purposes unrelated to the provision of care.[315] The Administration contends that this approach would also avoid the imposition of significant

310. *See* OTA, *supra* note 12, at 73.

311. *See id.* There are four generally accepted requirements for valid informed consent to medical treatment: "the act of consent must be genuinely *voluntary*, and there must be adequate *disclosure* of information to the patient about what is to be done. Patients must *comprehend* what they are being told . . . and be *competent* to consent." *Id.* at 70.

312. *See* GEORGE J. ANNAS, THE RIGHTS OF PATIENTS: THE BASIC ACLU GUIDE TO PATIENT RIGHTS 185 (2d ed. 1989); AHIMA, Resolve to Protect Health Information Confidentiality in 1998, at 1 (Dec. 29, 1997) (press release) (on file with the *North Carolina Law Review*).

313. *See, e.g.*, H.R. 1815, 105th Cong. §§ 202-203 (1997).

314. *See* HHS RECOMMENDATIONS, *supra* note 155, at 42-44. HHS had advocated a similar approach during previous health confidentiality debates. *See Hearings on S. 1360*, *supra* note 54, at 97 (statement of Nan Hunter, Deputy General Counsel, HHS). In its 1997 report to HHS, the NCVHS agreed with the statutory approach. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 8-9. This approach is already in use in several states, including California, *see* CAL. CIV. CODE § 56.10(a), (c)(1)-(3) (West 1982 & Supp. 1998), Montana, *see* MONT. CODE ANN. § 50-16-529(1)-(3) (1997), and Washington, *see* WASH. REV. CODE ANN. § 70.02.050(1)(a)-(c) (West 1992 & Supp. 1998).

315. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 9.

administrative burdens on the routine practice of health care.[316] Physicians could disclose necessary information to other providers, such as a specialist to whom the patient is referred, without having to obtain written consent, and authorization would not be required for the transmission of information between providers and third-party payers.[317] Because many different electronic claims processors may handle the flow of computerized information between provider and payer, and because the identity of these organizations cannot necessarily be determined in advance,[318] it would be difficult, the Administration asserts, for providers to satisfy the requirements of a valid authorization under any proposed legislation.[319] The Administration's plan would also provide an "opt-out" provision. Patients could prohibit the disclosure of certain information for treatment or payment purposes or could restrict the disclosure of this information to certain persons.[320]

While managed care organizations support the statutory authorization concept,[321] doctors and privacy advocates have expressed serious concerns.[322] The Administration's proposal runs counter to the principle of informed consent, they argue, because it implies that affirmative consent is essentially meaningless and thus an unnecessary burden for providers and payers who believe they have a "right" to patients' information.[323] Furthermore, they contend, the statutory authorization plan would be no less burdensome than

316. *See* HHS RECOMMENDATIONS, *supra* note 155, at 43.

317. *See id.*

318. *See Hearings on S. 1360*, *supra* note 54, at 107 (statement of Jeanne Schultz Scott on behalf of the Association for Electronic Health Care Transactions).

319. *See id.* at 110. Most health confidentiality legislation imposes detailed requirements for each valid authorization request, including a specification or description of the information to be disclosed, the purpose of the disclosure, the entity or individual to whom the data will be disclosed, and subsequent disclosures that the recipient intends to make. *See, e.g.*, H.R. 1815, 105th Cong. § 202(a) (1997). HHS suggested that forcing providers and payers to meet these requirements each time information is transmitted by electronic claims agents would "bring the health care payment system to a halt." HHS RECOMMENDATIONS, *supra* note 155, at 43.

320. *See* HHS RECOMMENDATIONS, *supra* note 155, at 43-44.

321. *See Privacy in the Electronic Age Hearings*, *supra* note 75, at 90-92 (prepared statement of John T. Nielsen on behalf of the American Association of Health Plans) (suggesting ways in which the statutory authorization proposal could be improved to assist managed care organizations).

322. *See id.* at 103 (prepared statement of Donald J. Palmisano on behalf of the American Medical Association); *id.* at 111 (prepared statement of Wanda Walker on behalf of the Consortium for Citizens with Disabilities); *id.* at 132 (prepared statement of the American Psychiatric Association).

323. *Id.* at 103 (prepared statement of Donald J. Palmisano on behalf of the American Medical Association).

current practice because permitting patients to "opt out" will be effective only if the provider enumerates all possible kinds of disclosures.[324] While acknowledging problems associated with "ritualized" patient authorizations, these groups assert that codifying authorization is not the best, or even a proper, way to address this issue.[325]

2. Disclosure for Research Purposes

One of the most contested areas in the confidentiality debate is access by researchers to individuals' health information. Within this issue, certain sub-issues are largely settled. Most proposals for a uniform federal law agree that researchers should be required, as soon as possible, to remove all identifiers from the health data they receive unless an institutional review board ("IRB")[326] permits retention.[327] The proposals also restrict researchers' ability to redisclose personally identifiable information. For example, broad consensus exists among legislators and interested groups that information obtained for research purposes should not be used against a record-subject in any administrative, civil, or criminal

---

324. *See id.*; *id.* at 111 (prepared statement of Wanda Walker on behalf of the Consortium for Citizens with Disabilities).

325. *See id.* at 103 (prepared statement of Donald J. Palmisano on behalf of the American Medical Association).

326. Every proposed research project involving human subjects that is conducted, funded, or regulated by a federal agency must receive the approval of an IRB. *See* 45 C.F.R. § 46.109 (1997). The purpose of an IRB is to "safeguard[] the rights and welfare of human subjects" through external oversight of research projects. *Id.* § 46.107(a). Each IRB must consist of at least five persons drawn from varying backgrounds. *See id.* At least one of the five must have a scientific background and at least one must have a non-scientific background. *See id.* § 46.107(c). At least one member must not be affiliated with the research institution to which the IRB is attached. *See id.* § 46.107(d). To approve a proposed research project, the IRB must determine that risks to the human subjects have been minimized; the risks are "reasonable in relation to [the] anticipated benefits" of the research; the selection of the human subjects is equitable; informed consent has been obtained; and, adequate precautions have been taken to protect the confidentiality of the human subjects and the data about them. *Id.* § 46.111. Many private sector institutions engaged in human research have established IRBs that follow similar guidelines. *See* LOWRANCE, *supra* note 66, at 41. There are approximately 3500 IRBs in the United States today. *See id.* For criticism of IRBs, see *infra* notes 347-48 and accompanying text.

327. *See* S. 1368, 105th Cong. § 222(h)(1) (1997); H.R. 1815, 105th Cong. § 210(d)(1) (1997); HHS RECOMMENDATIONS, *supra* note 155, at 52. There are several reasons why an IRB might permit a researcher to retain identifiers: questions may arise about the integrity of the research, follow-up research may be needed, or analysis of pharmaceutical and medical device side effects may be required. *See Hearings on H.R. 52*, *supra* note 27, at 119 (statement of the Pharmaceutical Research and Manufacturers of America); LOWRANCE, *supra* note 66, at 36.

proceeding.[328]

The principal issue that remains unsettled is whether researchers should be required to obtain an individual's informed consent to access identifiable data about that individual. Federal regulations already govern research involving human subjects that is conducted, supported, or regulated by federal agencies.[329] These regulations, collectively known as the Federal Common Rule ("Common Rule"), generally require researchers to obtain an individual's informed consent before conducting research involving that individual.[330] There are, however, limitations on this requirement. The regulations do not apply if the research involves only "the collection or study of existing data, documents, [or] records" about the individual and the information is publicly available or recorded in such a way that the identity of the individual cannot be directly or indirectly determined.[331] Even if the last two conditions are not met, informed consent is still not required if an IRB waives the requirement after finding that the research poses only minimal risk to the individual; failure to obtain consent will not "adversely affect the rights and welfare" of the individual; obtaining consent would be impractical; and, if possible, the individual will be notified at a later time.[332]

Several approaches to the informed consent issue have been proposed. One alternative is to incorporate the Common Rule or its principles in the health confidentiality statute. Senator Jeffords would permit non-consensual disclosure of data only to research projects conducted or supported by a federal agency that comply with the Common Rule itself,[333] while the Clinton Administration would

328. *See, e.g.*, S. 1368 § 222(i); H.R. 1815 § 210(d)(2); H.R. 52, 105th Cong. § 116(b)(2) (1997); HHS RECOMMENDATIONS, *supra* note 155, at 52. The House Committee on Government Operations asserted that "[t]his absolute protection is an essential part of the bargain that permits use of records by researchers." H.R. REP. NO. 103-601, pt. 5, at 126 (1994). For discussion of law enforcement's demands for health information, see *infra* notes 415-17 and accompanying text.

329. *See* Basic HHS Policy for Protection of Human Subjects, 45 C.F.R. §§ 46.101-.124 (1997). Similarly, research regulated by the Food and Drug Administration is governed by 21 C.F.R. §§ 50.1-.27, 56.101-.124 (1997).

330. *See* 45 C.F.R. § 46.116.

331. *Id.* § 46.101(b)(4).

332. *Id.* § 46.116(d).

333. *See* S. 1921, 105th Cong. § 208(a)(1) (1998). The Jeffords bill would also permit disclosure of data to research projects that are "not subject to the Federal Policy for the Protection of Human Subjects." *Id.* § 208(a)(3). Because research not conducted, funded, or regulated by the federal government falls outside the Policy, *see* 45 C.F.R. § 46.101(a), the Jeffords bill would apparently allow non-consensual disclosure of health information, without any showing of need, to research projects that are completely privately funded and not subject to government regulation.

permit non-consensual disclosure of data to all research projects, federally funded or otherwise, which comply with principles derived from the Common Rule.[334] The Administration recommends, for example, that the non-consensual disclosure of identifiable health data be permitted if conducting the research with anonymized data would be impractical; the research project has been approved by an IRB "organized and operated in a manner consistent with" the Common Rule; and the IRB has determined that consent is not necessary because the benefits of the project outweigh the privacy intrusion, the research poses minimal risk, the failure to obtain consent does not "adversely affect the rights and welfare" of the individuals, and obtaining consent would make it impractical to carry out the research.[335]

An alternative approach incorporates both outside review and a contractual obligation. Representative Shays's proposal would permit the non-consensual disclosure of archival health information,[336] so long as the researcher's request for the data is approved by a "board, committee, or other group formally designated by the [data holder] to review requests for such information, in accordance with written standards for confidentiality that specify permissible and impermissible uses of such information for health research," and the data holder "enters into a written agreement with the health researcher" that mandates compliance with Shays's other proposed re-disclosure and use restrictions.[337] A breach of the agreement "may provide a basis for civil action against the researcher" or could result in "other adverse consequences."[338] As Representative Shays has not defined what a "board, committee, or other group" and "other adverse consequences" are, it is not clear what kind of protection this proposal would offer to archived data,

334. Senator Leahy has taken a similar approach but would use regulations promulgated by HHS. *See* S. 1368, 105th Cong. § 222(a) (1997). He would also require the Secretary of HHS to report back to Congress after one year with recommendations concerning the advisability of requiring informed consent. *See id.* § 222(b).

335. HHS RECOMMENDATIONS, *supra* note 155, at 52. Representative Condit's latest proposal would impose a similar requirement. *See* H.R. 52, 105th Cong. § 116(a) (1997).

336. "Archival" patient information is that which was "previously created or collected by the [data holder] and maintained by the [data holder] in an archive or other repository." H.R. 3900, 105th Cong. § 106(a) (1998). It is not clear that this explanation provides a clear distinction between "archived" information and other data, for which the Shays proposal would require traditional IRB approval for non-consensual disclosure. *See id.* § 101(1)(B)(vi)(I). For instance, would "archived" data include data that have been held for only one week—or even one day?

337. *Id.* § 106(a)(2), (3).

338. *Id.* § 106(a)(4).

though it is certainly possible that it would be even less than that conferred by the IRB process.[339]

A final approach, one supported by patient-rights groups and the privacy community, is to forbid outright the non-consensual use of identifiable health data for research purposes.[340] Advocates advance three arguments in support of a consent requirement. First, the purported need for individually identifiable information for health research is questionable; much health research can be accomplished by using aggregated data without patient identifiers, so easy access to identifiable data is not justified.[341] Second, the principle of individual autonomy dictates that informed consent is a necessary predicate for all health research involving humans, including that which uses only records.[342] The first element of the Nuernberg Code, one advocate has noted,[343] stipulates that in medical research, "[t]he voluntary consent of the human subject is absolutely essential."[344] Failure to require patient authorization, this advocate has agreed, threatens the "constitutional guarantees of individual liberty."[345] Finally, privacy advocates argue that privacy is too important a right for its protection to be left to IRBs.[346] These committees are normally affiliated with the researcher's organization and are "likely to share the

339. Privacy advocates have criticized the Shays proposal for this very reason. *See* ACLU, *supra* note 193, at 1. The Shays proposal raises, and apparently provides one answer to, the question whether patients have a lesser privacy interest in old information—which is presumably "archived"—than in current information.

340. *See* H.R. 1815, 105th Cong. § 210(a) (1997) (sponsored by Rep. McDermott); Letter from Laura W. Murphy, Director, ACLU, to Senator Robert Bennett 1 (Oct. 27, 1995) (on file with the *North Carolina Law Review*).

341. *See Hearings on S. 1360*, *supra* note 54, at 86 (statement of the Public Citizen's Health Research Group).

342. *See, e.g.*, James Pyles, Testimony on Behalf of the National Coalition for Patient Rights Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 84 (Jan. 13, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) (arguing for a consent requirement because "there is very little difference between asking a person directly and getting the information indirectly"). *But see* PRIVACY COMMISSION, *supra* note 19, at 309 (noting that the argument for requiring patient authorization for use of health records for research "has always seemed less compelling" than the obligation to obtain consent for research on humans).

343. *See* Nagel Statement, *supra* note 193, at 4.

344. 2 NUERNBERG MILITARY TRIBUNALS, TRIALS OF WAR CRIMINALS BEFORE THE NUERNBERG MILITARY TRIBUNALS UNDER CONTROL COUNCIL LAW NO. 10, at 181-82 (1946-49).

345. Denise M. Nagel, Testimony on Behalf of the National Coalition for Patient Rights et al. Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 4 (Feb. 19, 1997) (unpublished transcript, on file with the *North Carolina Law Review*).

346. *See Hearings on S. 1360*, *supra* note 54, at 87 (statement of the Public Citizen's Health Research Group).

[researcher's] values concerning the importance of research at the expense of personal privacy."[347] Furthermore, observers note, IRBs have questionable experience addressing privacy issues because confidentiality of data has traditionally not been their primary concern.[348]

Health researchers respond that there is a legitimate need to access non-anonymized data. Research sometimes requires individually identifiable data[349] or, more frequently, data that are linkable to a specific individual.[350] These identifiers and linkages enable researchers to avoid duplication of records and to track the progress of an individual's medical condition or the consequences of treatment over time.[351] Researchers also claim that requiring consent to access these records will impede beneficial research.[352] Obtaining consent can be impractical if not impossible in many cases. Research often involves hundreds or even thousands of health records; tracking down every individual to obtain authorization would be an enormous burden.[353] In many cases, research is conducted retrospectively, and consent cannot be obtained because individuals have died or can no

347. *Id.* There is some support for this criticism. *See* H.R. REP. NO. 103-601, pt. 5, at 127 (1994) ("IRBs are not independent of the institutions that created them. The inherent conflict of interest is particularly strong when an IRB reviews research with commercial potential for the institution or company at which the IRB is located."). Only one member of an IRB must not be affiliated with the sponsoring institution. *See supra* note 326.

348. Even some supporters of non-consensual disclosure of data for research purposes concede that "IRBs have not historically focused on issues of confidentiality." *Hearing on S. 1368*, *supra* note 156, at 70 (statement of the Consortium for Citizens with Disabilities); *see also* LOWRANCE, *supra* note 66, at 42 (questioning whether IRBs "have been attending as vigorously to privacy risks as they have to physical and emotional risks"). *But see* Hoge Testimony, *supra* note 166, at 58 (arguing that IRB's have done "a wonderful job . . . protecting patients"); Donald J. Palmisano, Statement on Behalf of the American Medical Association Before Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 58 (Feb. 18, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Palmisano Statement] (suggesting that most researchers and patients are "generally satisfied" that IRBs provide adequate protection for the confidentiality of health information).

349. *See Hearing on S. 1368*, *supra* note 156, at 80 (statement of the Biotechnology Industry Organization).

350. *See, e.g.*, David Korn, Testimony on Behalf of the Association of American Medical Colleges Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 13, 15 (Jan. 13, 1997) (unpublished transcript, on file with the *North Carolina Law Review*).

351. *See, e.g.*, LOWRANCE, *supra* note 66, at 36.

352. *See, e.g.*, Robert A. Hiatt, Testimony on Behalf of the American College of Epidemiology Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 6-7 (Jan. 13, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Hiatt Testimony].

353. *See* HHS RECOMMENDATIONS, *supra* note 155, at 54.

longer be located.[354] The unavailability of these records could raise doubts about the strength of the research. Because those individuals who could not be located might differ in some significant respect from those whose records are included, respondent bias might compromise the research results.[355] The same problem would occur, researchers claim, if individuals who could be found refused to provide consent.[356]

After considering arguments on the informed consent issue from both researchers and privacy advocates, the NCVHS concluded that an absolute consent requirement would not be advisable,[357] stating its belief that to impose such a requirement would add an "impractical and expensive" burden on researchers and, consequently, would significantly reduce the amount of research conducted for the ultimate benefit of the public.[358] The Committee cited the requirement of prior IRB approval, the prohibition on using the data against the individual in administrative and criminal proceedings, and a requirement that researchers remove all identifiers when feasible as sufficient to protect patient privacy.[359]

3. Disclosure for Public Health Purposes

Confidentiality issues pertaining to public health data engender somewhat less controversy than those that surround the use of data by medical researchers.[360] A probable explanation for this distinction is that the concept of public health is less abstract than traditional research and its benefits are more easily visualized.[361] The public is

354. *See Privacy in the Electronic Age Hearings*, *supra* note 75, at 71-72 (statement of Elizabeth B. Andrews, M.D., on behalf of the Healthcare Leadership Council); HHS RECOMMENDATIONS, *supra* note 155, at 54. One prominent example of retrospective research in recent years involved an investigation into why young women were developing a rare form of vaginal cancer at 15 to 20 years of age. The investigation required researchers to track down and access the mothers' medical records to determine what drugs, if any, were used during pregnancy. The drug DES was identified as the cause of the cancer. According to researchers, this investigation would have been difficult to complete had the mothers' consent been required. *See* H.R. REP. NO. 103-601, pt. 5, at 121 (1994).

355. *See, e.g.*, Hiatt Testimony, *supra* note 352, at 7.

356. *See, e.g.*, *id.* at 12. To explain respondent bias, Dr. Hiatt drew an analogy to reactions to phone calls from direct marketers: some persons will hang up—that is, they do not consent to participate—while others listen. Those who hang up, Dr. Hiatt noted, are different from those who choose to listen. *See id.*

357. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 12.

358. *Id.*

359. *See id.*

360. *See id.* at 13.

361. *See id.*

more likely to support the use of personally identifiable data for public health functions than for traditional medical research,[362] and the deferential treatment accorded public health agencies is evident in many of the proposals for a federal confidentiality law.[363]

While aggregated data are often sufficient for public health purposes, agencies must frequently use personally identifiable information to carry out certain functions.[364] Charged with creation of an official public record, public health agencies monitor and record births, deaths, marriages, divorces, and other vital statistics.[365] In compliance with state reporting laws, they collect reports provided by doctors and hospitals of certain communicable diseases and other health conditions.[366] In addition to the passive collection of data, agencies conduct public health surveillance, looking proactively for emerging diseases and outbreaks of disease, patterns of morbidity, and trends in risky behaviors.[367] As a result of their data collection and surveillance duties, agencies must sometimes use identifiable information to act affirmatively for the public health. For example, an agency may be authorized by law to contact individuals who may have been exposed to communicable diseases so that appropriate treatment can be administered.[368]

---

362. *See id.*

363. *See infra* notes 386-89 and accompanying text.

364. *See* H.R. REP. NO. 103-601, pt. 5, at 119 (1994).

365. *See, e.g.*, David Fleming, Testimony on Behalf of the Council of State and Territorial Epidemiologists Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 40 (Jan. 13, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Fleming Testimony].

366. All 50 states have enacted statutes that require health care providers to report certain individually identifiable data to public health authorities; consent of the patient is not required. *See* GOSTIN ET AL., *supra* note 143, at 27-28, 34. Traditionally, these "reporting statutes" were grouped into four categories: birth and death statistics, infectious and communicable diseases, child abuse, and gunshot and pointed object wounds. *See* WESTIN, *supra* note 191, at 21-22. States continue to add new reporting requirements, such as laws mandating reports of elder abuse. *See* Schwartz, *supra* note 12, at 321.

367. Surveillance is one of the oldest functions of public health. *See* LOWRANCE, *supra* note 66, at 22. Increasingly, the scope of surveillance extends beyond the traditional identification of disease to include environmental risks and personal behaviors such as smoking, drug use, and use of seatbelts. *See* GOSTIN ET AL., *supra* note 143, at 28.

368. *See, e.g.*, Fleming Testimony, *supra* note 365, at 40-41. For example, 37 states have laws providing for the notification of a spouse or partner of possible exposure to a sexually transmittable disease. *See* GOSTIN ET AL., *supra* note 143, at 36. Those so notified are normally not informed of the identity of the source of possible exposure. *See id.* at 82. For analysis of confidentiality issues pertaining to notification of possible HIV exposure, see *id.* at 82-89; Lawrence O. Gostin & James G. Hodge, Jr., *Piercing the Veil of Secrecy in HIV/AIDS and Other Sexually Transmitted Diseases: Theories of Privacy and Disclosure in Partner Notification*, 5 DUKE J. GENDER L. & POL'Y 9 (1998). For an

Protection of public health has traditionally been a duty of the states.[369] Identifiable data about individuals are, however, increasingly collected and maintained in regional and national public health databanks.[370] As one report has noted, "[t]he development of a public health information infrastructure is not a distant concept, but an emerging reality."[371] The U.S. Public Health Service, for example, is developing an automated system that will link state databases across the country,[372] and several federal agencies are collaborating in the National Health and Nutrition Examination Survey ("NHANES"), which has been described as the "most ambitious public effort to create a population-based database."[373] In the latest round of NHANES, more than 8000 pieces of health-related data will be collected from each of approximately 30,000 individuals through interviews and examinations.[374] Public health experts analyze the data concerning these individuals in an effort to improve health outcomes for the larger population in the United States and abroad.[375] The data collected through the survey are subject to strict federal confidentiality protections, including a prohibition on redisclosure of identifiable information without the consent of the individual.[376] If consent is given, disclosure is permitted only to other federal agencies.[377]

Reflecting the predominant state role in public health, most existing confidentiality protections concerning public health data have been enacted or promulgated at the state level.[378] The 1996 survey of state health confidentiality laws found a patchwork of often dissimilar rules. Every state but one has created statutory or regulatory protection for public health information generally, and forty-two states have specific protections for communicable diseases

---

analysis and recommendations concerning the confidentiality of HIV-related information in the public health context generally, see Roger Doughty, Comment, *The Confidentiality of HIV-Related Information: Responding to the Resurgence of Aggressive Public Health Interventions in the AIDS Epidemic*, 82 CAL. L. REV. 111 (1994).

369. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 13.

370. *See* GOSTIN ET AL., *supra* note 143, at 29.

371. *Id.* The "public health infrastructure" is defined as the "framework that undergirds the electronic information collection, storage, use, and transmission supporting the essential functions of the public health system." *Id.* at 16.

372. *See id.* at 29.

373. *Id.* at 29-30.

374. *See* LOWRANCE, *supra* note 66, at 24.

375. *See id.*

376. *See id.*

377. *See id.*

378. *See* GOSTIN ET AL., *supra* note 143, at 1-6.

and sexually transmitted diseases.[379] These statutes and regulations differ dramatically in the ease with which they permit redisclosure of data.[380]

Despite these discrepancies, public health officials have expressed concern about replacing the present system of state laws with uniform federal guidelines.[381] They note that decisions concerning the balance between individual privacy and public health needs have traditionally been made at the state level and argue that this tradition should continue.[382] Citing their excellent track record of safeguarding data, officials suggest that the existing system of state public health confidentiality laws works well.[383] Although reporting, surveillance, and confidentiality guidelines vary from state to state, public health agencies are comfortable with the long-standing laws that currently apply in their respective states.[384] Any effort to impose new federal rules designed to alter significantly the status quo would, they argue, "create a fair amount of at least temporary chaos" in the public health community.[385]

All of the proposals for a uniform federal law would provide baseline standards for confidentiality protection, and to the extent that existing state laws concerning public health data do not meet these standards, the federal law would preempt state law.[386] Mindful, however, of the traditional role of states in protecting the public health, the proposals make allowances for state public health laws. Under almost all proposals, even those that would otherwise impose

379. *See id.* at 33-34.

380. *See id.* at 37-38.

381. *See* Fleming Testimony, *supra* note 365, at 41. *But see* Gellman, *supra* note 87, at 148 (suggesting that there has been "no visible opposition" to federal preemption by state agencies).

382. *See* Fleming Testimony, *supra* note 365, at 41.

383. *See id.* Public health agencies have established a commendable record of safeguarding the individually identifiable data they receive. *See* H.R. REP. NO. 103-601, pt. 5, at 120 (1994). One dramatic exception to this record occurred in Tampa, Florida, in 1996, when a state employee copied the names of almost 4000 HIV positive and AIDS patients from a Pinellas County Health Department computer to a disk and mailed the disk to two major newspapers. *See* Sue Landry, *AIDS List Is Out—State Investigating Leak*, ST. PETERSBURG TIMES, Sept. 20, 1996, at A1.

384. *See* Fleming Testimony, *supra* note 365, at 55 (arguing that a federal confidentiality law "could create a lot of problems at the individual state level" for public health because "rules, regulations, [and] practices ... have evolved around how the [state] laws are currently worded").

385. *Id.*

386. *See, e.g.*, S. 1921, 105th Cong. § 401(a)-(c) (1998); S. 1368, 105th Cong. § 401(a) (1997); H.R. 1815, 105th Cong. § 402(a) (1997); HHS RECOMMENDATIONS, *supra* note 155, at 15-17.

a "ceiling" on confidentiality protections, more stringent state laws concerning public health functions would be exempt from the federal confidentiality statute.[387] This deferential treatment of existing state-level protections reflects not only the wishes of state public health officials but also the position of the privacy community. Privacy advocates insist that a comprehensive federal law must permit states to pass more stringent confidentiality laws generally, including laws protecting public health data.[388] An obvious beneficiary of this approach is HIV-related information, which already enjoys stringent confidentiality protection in some states, in certain cases surpassing anything proposed at the federal level.[389]

According to privacy advocates, the need for states to create stronger protections is underscored by what the advocates claim are the inadequate confidentiality requirements some proposals would impose on public health agencies.[390] The Clinton Administration's recommendations, for example, would give public health agencies broad access to identifiable health information. Non-consensual disclosure of data to public health agencies would be permitted for any lawful "disease or injury reporting, public health surveillance, or public health investigation or intervention."[391] Privacy advocates claim that such a proposal would make it too easy for public health agencies to obtain identifiable information because agencies would not be required to demonstrate a need for the data.[392] Some advocates have even argued that non-consensual access be strictly limited to situations in which the public health agency can establish a "specific nexus" between the need to obtain identifiable information and a threat of harm or death to one or more persons.[393] While the

387. *See, e.g.*, S. 1368 § 401(a); H.R. 1815 § 402(a); S. 1360, 104th Cong. § 401(a), (c)(1), (c)(3) (1995).

388. *See infra* notes 504-11 and accompanying text.

389. *See* GOSTIN ET AL., *supra* note 143, at 77; *see also* Robert Gellman, Testimony Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 55 (Jan. 13, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Gellman Testimony] (suggesting that the exception from preemption for state public health laws "was an attempt to leave state AIDS laws alone").

390. *See, e.g.*, *Hearings on S. 1360*, *supra* note 54, at 145 (statement of the Consumer Project on Technology).

391. HHS RECOMMENDATIONS, *supra* note 155, at 48. Senator Bennett's health confidentiality legislation in the 104th Congress contained a similar provision. *See* S. 1360 § 208 (1995).

392. *Cf. Hearings on S. 1360*, *supra* note 54, at 87 (statement of the Public Citizen's Health Research Group) (criticizing a similar provision in S. 1360 for not requiring public health agencies to show why they need identifiable data).

393. Memorandum from Chai Feldblum & Janlori Goldman to Working Group on S.

more stringent legislative proposals have incorporated the "specific nexus" concept, they do not attempt to define what it means;[394] it is unclear how much more restrictive such a requirement would be in practice.[395] Furthermore, recent proposals vary dramatically on the issue of subsequent disclosure of data by public health agencies, from imposing no restrictions to permitting disclosures only for purposes related to public health reporting, surveillance, investigation, and intervention.[396]

4. Disclosure for Oversight Purposes

Access to identifiable health data by oversight organizations remains one of the most contentious issues in the effort to enact a federal law.[397] Functions traditionally associated with oversight include cost containment efforts, quality assurance reviews, utilization of resource studies, anti-fraud investigations, licensure of physicians and other providers, and accreditation of health care institutions.[398] Accrediting bodies, such as the Joint Commission on Accreditation of Healthcare Organizations, and licensing bodies, such as state medical boards, are important mechanisms for ensuring certain standards of proficiency and safety in the provision of care.[399] Oversight activities are also a principal means for curbing spiraling health care costs, particularly when these costs are driven by fraud and waste. HHS conducts audits, for example, to detect abuses of the Medicare and Medicaid programs.[400] Similarly, law enforcement agencies and state insurance commissioners investigate charges of overbilling and other forms of fraud.[401] While oversight activities often require only anonymized or aggregated data, access to individually identifiable patient records is frequently necessary.[402]

1360, *supra* note 230, at 9 (noting such a proposal by the ACLU of Massachusetts).

394. S. 1368, 105th Cong. § 212(a) (1997); H.R. 1815, 105th Cong. § 209(a) (1997).

395. *Cf.* NCVHS RECOMMENDATIONS, *supra* note 185, at 13 (characterizing public health access provisions in most proposals as "broad and mostly undefined").

396. S. 1360, introduced in the 104th Congress, would have imposed no restrictions on the further use or disclosure of data by public health agencies. *See* S. 1360 § 208. The Administration recommends that subsequent disclosures be limited to health care, public health, research, and oversight purposes. *See* HHS RECOMMENDATIONS, *supra* note 155, at 49. The most recent McDermott bill would limit redisclosures to purposes of public health reporting, surveillance, investigation, and intervention. *See* H.R. 1815 § 209(c).

397. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 13.

398. *See* HHS RECOMMENDATIONS, *supra* note 155, at 45-46.

399. *See, e.g.*, OTA, *supra* note 12, at 47.

400. *See, e.g.*, HHS RECOMMENDATIONS, *supra* note 155, at 46.

401. *See id.*

402. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 13.

Legislative proposals vary in the extent to which they would permit disclosure of data for oversight purposes. Many proposals, including the Clinton Administration's recommendations, assert a legitimate need for access by permitting non-consensual disclosure in certain situations,[403] but many privacy advocates strenuously object and call for a consent requirement or at least notice to the patient.[404] The privacy community has also criticized previous proposals for defining "oversight" broadly, arguing that an expansive definition will permit an indeterminable number of organizations to access data.[405] There is some basis for this criticism. Because oversight activities "are hard[] to classify or even identify," the NCVHS found that legislative proposals usually define the term loosely for fear that a legitimate activity will be excluded.[406] An expansive definition of "oversight" can be problematic because, under all proposals, the ability to access data without consent depends on the use to which the data will be applied. If a purpose appears to qualify for more than one category of use as defined by the legislation, which confidentiality rules apply?[407]

An example of this problem in the health oversight context is the

403. *See, e.g.*, S. 1368, 105th Cong. § 214 (1997); H.R. 1815, 105th Cong. §§ 207-208 (1997); S. 1360, 104th Cong. § 206 (1995); HHS RECOMMENDATIONS, *supra* note 155, at 44-45.

404. *See, e.g., Hearings on S. 1360*, *supra* note 54, at 145 (statement of the Consumer Project on Technology). The Clinton Administration has recommended that non-consensual disclosure of identifiable data be permitted if authorized by any other law "for oversight of the health care system." HHS RECOMMENDATIONS, *supra* note 155, at 44. Other legislative proposals are significantly more restrictive. For example, one proposal would require a showing of probable cause that fraud has been committed and that the individually identifiable data are necessary to investigate this fraud, or that the data are necessary to investigate possible incidents of "abuse, neglect, or exploitation of an individual." H.R. 1815 § 207(a). This proposal would also require oversight agencies to notify "at the first practical opportunity" individuals who are not the targets of an investigation that their health records have been accessed and to explain the reasons for unconsented access. *Id.* § 207(c).

405. *See Hearings on S. 1360*, *supra* note 54, at 87 (statement of Public Citizen's Health Research Group).

406. NCVHS RECOMMENDATIONS, *supra* note 185, at 13. A typical definition of an oversight agency is one who "performs or oversees the performance of an assessment, investigation, or prosecution relating to ... compliance with legal or fiscal standards pertinent to health care fraud ... [or] the protection of individuals from harm, abuse, neglect, or exploitation" and is a public agency, acts on behalf of an agency, acts in compliance with an agency requirement, or acts with authorization of federal or state law. H.R. 1815 § 3(8).

407. It has been suggested that users of health information will attempt to characterize themselves "in the most benign manner" so that they will face the least stringent access requirements possible. *Hearings on H.R. 52*, *supra* note 27, at 62 (statement of the American Medical Association).

HHS Inspector General, who is responsible for investigating fraud in the Medicare and Medicaid programs.[408] Pursuant to this responsibility, the Inspector has the statutory power to compel by subpoena the production of any individual's health record.[409] However, because the Inspector uses information contained in these records to aid criminal prosecutions for fraud, it is unclear whether exercising this power would be considered an "oversight" or a "law enforcement" activity for purposes of the confidentiality law.[410] Although it may be impossible to draw such a distinction in practice, legislative proposals attempt to do so in theory, and the result is uncertainty as to which procedures must be followed to access identifiable health information without consent—those applicable to oversight agencies or those applicable to law enforcement.[411] This problem led the NCVHS to caution that "treating so many different functions and users under the same 'oversight' category should be avoided" and that "[m]ore study is needed to draw useful distinctions between [oversight and other] activities and to find better and narrow[er] definitions of legitimate uses and users."[412] The Clinton Administration's response to the Inspector General problem is to require investigative agencies and officials to continue to satisfy existing access procedures stipulated by statute as a prerequisite to compelling the production of records.[413] As discussed in the following section, however, this requirement provides little comfort to privacy advocates.[414]

5. Disclosure for Law Enforcement Purposes

Law enforcement agencies seek access to identifiable health information primarily for two purposes. First, agencies and prosecutors rely on individual patient records when investigating

408. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 13.

409. *See* Inspector General Act of 1978, 5 U.S.C. app. § 6(a)(4) (1994).

410. *See* H.R. REP. NO. 103-601, pt. 5, at 90 (1994) (noting that the Inspector General has both "oversight and law enforcement roles" and that detection of fraud will lead to "criminal and civil prosecutions and administrative sanctions").

411. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 14.

412. *Id.* As one congressional staff aide has observed, definitional issues are the source of " 'ninety percent' " of the unresolved disagreements related to a health confidentiality law. *Records Privacy Law Won't Be Done This Congress, Hill Aides Say*, HEALTH LEGIS. & REG. WKLY., Jan. 21, 1998, *available in* 1998 WL 10395658 (quoting an unidentified congressional staff member).

413. *See* HHS RECOMMENDATIONS, *supra* note 155, at 48.

414. *See infra* notes 429-33 and accompanying text (discussing criticism of law enforcement's present ability to access health information).

potential cases of fraud in the health care industry.[415] Although providers and payers are the usual targets of such investigations, patient records must be reviewed to confirm the fraudulent activity and to build a sufficient amount of evidence.[416] Second, law enforcement officials also use health information to further investigations of specific individuals unrelated to fraudulent activity.[417]

Law enforcement officials generally use compulsory process, in the form of a warrant or subpoena, to obtain patients' medical records.[418] States differ in their requirements for obtaining subpoenas, with some states requiring prior judicial approval to issue certain subpoenas and others imposing no such requirement.[419] Federal law enforcement officials use a search warrant when the party under investigation holds the information sought; otherwise, federal agents normally use grand jury subpoenas to access medical records.[420] To obtain a subpoena, federal law enforcement officials need only to convince a prosecutor that the information sought is relevant to the scope of a pending grand jury investigation.[421] Satisfied that the information is relevant, the prosecutor drafts and signs the subpoena, and law enforcement officials serve it.[422] No judicial oversight is required unless the recipient of the subpoena refuses to disclose the information, in which case officials must seek a

415. *See* Robert S. Litt, Deputy Assistant U.S. Attorney General, Prepared Statement on Behalf of the U.S. Department of Justice Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 1 (Feb. 18, 1997) (unpublished statement, on file with the *North Carolina Law Review*).

416. *See id.*

417. *See id.* For example, in a hostage situation, police could access the captor's medical records to learn of any history of mental illness. *See id.* at 2.

418. *See* Robert S. Litt, Deputy Assistant Attorney General, Testimony on Behalf of the U.S. Dep't of Justice Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 10 (Feb. 18, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Litt Testimony].

419. *See id.* at 10-11.

420. *See id.* at 10. Depending on the nature of the investigation, an administrative subpoena may be used instead of a grand jury subpoena. *See* PRIVACY COMMISSION, *supra* note 19, at 367. Various statutes authorize federal agencies with investigative responsibilities to use subpoenas to compel the disclosure of information without prior judicial review. *See id.* For example, when investigating a health care offense, the U.S. Attorney General has statutory authority to demand by subpoena the disclosure of any medical record. *See* 18 U.S.C.A. § 3486 (West Supp. 1998). Administrative subpoenas raise privacy concerns similar to those raised by grand jury subpoenas. *See* PRIVACY COMMISSION, *supra* note 19, at 367-72.

421. *See* Litt Testimony, *supra* note 418, at 10.

422. *See id.*

court order to compel disclosure.[423] The recipient can then challenge the subpoena before the court on the basis of some legally protected interest in the requested information;[424] however, if the subpoena has been served on a third party (a doctor, for example) for the purpose of obtaining records pertaining to an individual patient, that patient may not have the necessary standing to issue a challenge.[425] The ability to challenge the subpoena is, moreover, predicated on knowledge of its existence. Grand jury subpoenas have no notice requirement, so patients may not be aware that law enforcement officials have obtained personal information from their doctor or hospital.[426] Finally, no guarantee exists that information obtained pursuant to the subpoena will even be used for the purpose for which it was obtained. Although evidence shown to a grand jury is sealed for secrecy, prosecutors sometimes choose not to show evidence to the grand jury.[427] If the health information is not sealed, law enforcement officials could potentially use it for other investigative purposes.[428]

The ease with which federal law enforcement officials obtain health information was criticized as early as 1977 by the Privacy Protection Study Commission ("Privacy Commission").[429] The Privacy Commission found that the subpoena had become "little more than an administrative tool" by which law enforcement could access individuals' records without having to satisfy the probable cause standard of a search warrant.[430] This criticism has since been echoed by at least one court[431] and noted by Congress.[432] The Privacy

423. *See* PRIVACY COMMISSION, *supra* note 19, at 366-67. The American Psychiatric Association urges its members to ignore subpoenas and to wait for a court order before turning over patient records. *See* Hoge Testimony, *supra* note 166, at 67.

424. *See* PRIVACY COMMISSION, *supra* note 19, at 366.

425. *See id.* As noted previously, the courts have been reluctant to recognize individuals' protected interest in information held about themselves by a third-party. *See supra* notes 119-23 and accompanying text (discussing *United States v. Miller* and its possible application to health-related information).

426. *See* PRIVACY COMMISSION, *supra* note 19, at 366-67.

427. *See id.* at 376-77; Litt Testimony, *supra* note 418, at 38. Law enforcement officials have expressed a willingness to accept a federal law that would require health records obtained by grand jury subpoena to be shown to the grand jury. *See* Litt Testimony, *supra* note 418, at 8. Federal law already imposes such a requirement for financial records obtained by grand jury subpoena. *See* 12 U.S.C. § 3420(a) (1994).

428. Use of the health information evidence by federal agencies would still be governed by the Privacy Act; however, as previously noted, the Act is riddled with exceptions. *See supra* notes 91-96 and accompanying text.

429. *See* PRIVACY COMMISSION, *supra* note 19, at 366-77.

430. *Id.* at 377.

431. *See* Thurman v. Texas, 861 S.W.2d 96, 101 (Tex. App. 1993, no writ) (Cohen, J., concurring) ("The unrestricted use of grand jury subpoenas to obtain medical records is a

Commission called for a statutory solution that would place stringent limitations on the use of grand jury subpoenas to access medical information.[433]

Heeding this recommendation, most health privacy legislative proposals have incorporated restrictions of varying strengths to access by law enforcement. Senator Bennett's initial proposal in 1995 would have imposed relatively modest restrictions, requiring law enforcement agencies to show probable cause that the desired health data are "relevant" to an investigation.[434] More recent proposals, however, would impose even more stringent requirements.[435] For example, legislation introduced by Senator Leahy would require law enforcement officials to obtain a court order to access health data and would condition this order on a showing by clear and convincing evidence that the records are "*necessary* to a legitimate law enforcement inquiry into *a particular* violation of criminal law," that the investigation cannot rely on non-identifiable data, and that the need to obtain the data "outweighs the privacy interest of the individual."[436]

Another feature common to confidentiality proposals is a requirement that the agency serve notice on the individual whose records are sought, either prior to the execution of the court order or subpoena or, in some proposals, within a specified time following execution, and that this individual have an opportunity to challenge access.[437] In some bills, the notice requirement could be excused if law enforcement could make an adequate showing that providing notice would risk the destruction of evidence.[438] Most bills would also prohibit the use of health-related information indicating criminal

---

serious threat to privacy. There is almost no limit on what can be obtained without the knowledge or approval of any court, any grand jury, . . . or the person affected.").

432. *See* H.R. REP. NO. 103-601, pt. 5, at 135-36 (1994).

433. *See* PRIVACY COMMISSION, *supra* note 19, at 378.

434. S. 1360, 104th Cong. § 212(a) (1995).

435. *See, e.g.*, S. 1368, 105th Cong. § 215(a)-(b) (1997); H.R. 1815, 105th Cong. § 213(b) (1997).

436. S. 1368 § 215(a)-(b) (emphasis added).

437. *See, e.g.*, S. 1368 § 215(c) (requiring prior notice to the individual unless the court determines that his whereabouts are unknown or there is a risk that the evidence is unavailable or will be destroyed); H.R. 1815 § 213(d)(3)-(4) (requiring a law enforcement agency to notify an individual within 30 days that the agency has obtained by warrant protected health information concerning that individual and permitting the individual to file a motion to quash); S. 1360 § 212(a)(3)-(4) (requiring a law enforcement agency to notify an individual within 30 days that the agency has obtained protected health information by warrant and requiring prior or concurrent notification if a subpoena or summons is used to obtain the information).

438. *See, e.g.*, S. 1368 § 215(c)(2).

activity by a patient against that patient if discovered during the course of an investigation not related to the criminal activity.[439]

Law enforcement officials have sharply criticized these proposals.[440] Introducing new restrictions on access, they charge, will unduly burden their efforts to obtain and use information necessary for investigations and successful prosecutions.[441] They claim, as an example, that a warrant requirement to obtain any health data would hamper investigations because officers often are unable to identify with necessary specificity the patient records sought.[442] Placing additional requirements on their ability to access records will also provide defense counsel with opportunities to attack collateral issues at trial such as procedural violations.[443] Furthermore, officials argue, it is a "perverse" idea to ignore evidence of patients' criminal activity found while investigating a provider or payer for fraud.[444] Rather than operate under these conditions, law enforcement officials demand a complete exemption from any health privacy legislation enacted by Congress.[445] The current system, officials assert, adequately protects patients' privacy rights.[446] In support of this proposition, officials note the absence of documented breaches of patient confidentiality[447] and suggest that there is little evidence to indicate that patients do not seek medical care out of fear of access to records by law enforcement.[448]

The Clinton Administration's proposal reflects law

---

439. *See, e.g., id.* § 215(e); H.R. 1815 § 213(c).

440. *See, e.g.*, Gallagher Testimony, *supra* note 36, at 3-4.

441. *See* Litt Testimony, *supra* note 418, at 8. *But see* PRIVACY COMMISSION, *supra* note 19, at 391 (arguing that law enforcement's "burden argument ... is not totally convincing").

442. *See, e.g.*, Mike Barnes, Testimony on Behalf of the National District Attorneys Association Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 5-6 (Feb. 18, 1997) (unpublished transcript, on file with the *North Carolina Law Review*).

443. *See* Litt Testimony, *supra* note 418, at 8.

444. *Id.*

445. *See* Gallagher Testimony, *supra* note 36, at 3.

446. *See* Litt Testimony, *supra* note 418, at 8. Personally identifiable information held by federal law enforcement agencies is protected by the Privacy Act of 1974, *see supra* notes 88-96 and accompanying text, but the Act contains many exemptions, and, in the view of one commentator, "every law enforcement agency ... has invoked every available exemption all the time." Robert Gellman, Chairman Statement, Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 19 (Feb. 18, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Gellman Statement].

447. *See* Litt Testimony, *supra* note 418, at 7.

448. *See id.* at 8.

enforcement's desire to retain the status quo.[449] Its plan would impose no new restrictions on law enforcement's ability to access, use, or redisclose identifiable health information.[450] Non-consensual disclosure of patient information to a law enforcement agency would be permitted as long as the agency "states that the health information is needed for a legitimate law enforcement inquiry" and complies with any other existing state or federal laws relating to access, such as having to obtain a subpoena or seeking prior approval of the courts.[451] Similar provisions would apply to access of health information by members of the intelligence community.[452] The Administration justifies not imposing new restrictions on the basis that "[t]hese disclosures are necessary to protect the health care system and the public, and they comport with certain well-accepted realities of law enforcement and the criminal justice system."[453] It argues that these recommendations strike the proper balance between competing public and private interests.[454]

Apparently, everyone but law enforcement disagrees with this position. Members of Congress, privacy advocates, and the health care industry have condemned the Administration's recommendations as a threat to patient privacy, arguing that the proposal would ensure that law enforcement retains unparalleled access to medical records.[455] Privacy advocates, in particular, are concerned that unless new restrictions are imposed, the increasingly prevalent use of computer networks and databanks to store health information will permit law enforcement agencies to search easily large quantities of patient records for evidence of criminal activity.[456]

---

449. *See* HHS RECOMMENDATIONS, *supra* note 155, at 60-61.

450. *See id.*

451. *Id.* at 60.

452. *See id.*

453. *Id.*

454. *See Privacy in the Electronic Age Hearings*, *supra* note 75, at 23-24 (prepared statement of Donna Shalala, Secretary of HHS).

455. *See, e.g.*, Janlori Goldman, Director, Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, Testimony Before the Senate Comm. on Labor and Human Resources 7 (Feb. 26, 1998) (unpublished transcript, on file with the *North Carolina Law Review*) (noting that the Administration's law enforcement proposal has garnered criticism from "[Capitol] Hill, the media, health care providers, and health privacy experts"); *The Outcry over HHS's Privacy Proposals*, HEALTH DATA NETWORK NEWS, Sept. 20, 1997, at 1-2 (discussing criticism of the Administration's law enforcement proposal by the ACLU, the American Hospital Association, and members of Congress). The result of the Administration's plan, one privacy advocacy quipped, would be that doctors should begin to read patients their Miranda rights. *See Privacy in the Electronic Age Hearings*, *supra* note 75, at 108 (prepared statement of A.G. Breitenstein).

456. *See, e.g.*, *Hearings on S. 1360*, *supra* note 54, at 142-43 (statement of the

In response to these criticisms, the Administration has attempted to shift the focus away from an absence of new restrictions to the proposed imposition of new criminal and civil penalties for misuse of health information by law enforcement.[457] These "severe" penalties will, it asserts, adequately strengthen privacy protections for the public.[458] The Administration has also downplayed critics' concerns about computerized fishing expeditions, responding that imposing restrictions on law enforcement's ability to search computerized databases of health records would be "premature" at this time because "more experience . . . with the nature and speed of computerization of these records" is needed.[459]

D. Use of Information by Employers

One issue not specifically addressed by many legislative proposals is access to and use of identifiable health data by employers.[460] In their roles as providers of employee health benefit plans, direct medical care, and wellness programs, employers frequently use or have access to employees' health data.[461] In an attempt to regulate costs, for example, self-insured employers monitor employee treatment and prescription claims approved by their benefit plan administrators.[462] Employers with in-house medical divisions provide medical care directly to their employees.[463] Many employers also require physical exams to determine that employees may safely carry out their jobs and conduct employee surveys as part

---

Consumer Project on Technology). For more vivid criticism on this point, see American Psychiatric Association, *supra* note 185, at 2 (equating the danger of surveillance of records by the "police 'paparazzi' " to "giving the police the right of hot pursuit through a crowded schoolyard"). For an argument why practical considerations will hinder law enforcement's ability to search computer databases, see Litt Testimony, *supra* note 418, at 16.

457. *See Privacy in the Electronic Age Hearings*, *supra* note 75, at 9 (testimony of Donna Shalala, Secretary of HHS) (responding to senators' concerns about law enforcement access by emphasizing that law enforcement officials "would be covered by the criminal penalties, and this is the important point that we've made here").

458. *Id.* at 15.

459. HHS RECOMMENDATIONS, *supra* note 155, at 61.

460. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 15.

461. *See Hearings on H.R. 4077*, *supra* note 48, at 328 (statement of Dr. Martin Sepulveda of IBM); Richard Kowalski, Testimony on Behalf of General Motors Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 4 (Feb. 3, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Kowalski Testimony].

462. *See Hearings on H.R. 4077*, *supra* note 48, at 328 (statement of Dr. Martin Sepulveda of IBM).

463. *See* Kowalski Testimony, *supra* note 461, at 3-4.

of wellness programs.[464] Employees are understandably concerned that employers will use these data for discriminatory purposes,[465] so much so that some workers ask their health care providers to falsify a diagnosis out of fear that their employer will obtain their record.[466]

Employers can effectively use health information in such a way as to protect employees' privacy.[467] For example, payments made by contract benefits administrators can be monitored using aggregated claims data, which do not link individual employees with particular medical conditions,[468] and in-house medical staff can explain to management that an employee-patient must miss work without revealing the specific medical reason or other protected health information.[469] Many employers have, in fact, voluntarily instituted internal guidelines designed to protect the confidentiality of employees' health data.[470] IBM, for example, has placed restrictions on how its contract benefits administrators can use its employees' health data and requires these administrators to pass treatment and prescription benefits information to the company in aggregated form only.[471] Similarly, General Motors has instituted a confidentiality policy that generally prohibits the disclosure of information obtained by its in-house medical staff without the authorization of the employee-patient.[472] Employers with such self-imposed confidentiality policies point out that these restrictions do not frustrate their efficiency or ability to do business.[473]

Such confidentiality practices are not, however, recognized by all employers. Some employers demand that their in-house medical

---

464. *See id.* at 4.

465. *See* HHS RECOMMENDATIONS, *supra* note 155, at 27.

466. *See Hearings on S. 1360*, *supra* note 54, at 64 (statement of Janlori Goldman, Deputy Director of the Center for Democracy and Technology).

467. *See* Kowalski Testimony, *supra* note 461, at 4-5.

468. *See Hearings on H.R. 4077*, *supra* note 48, at 330 (statement of Dr. Martin Sepulveda of IBM).

469. *See* Kowalski Testimony, *supra* note 461, at 4.

470. *See* PRIVACY COMMISSION, *supra* note 19, at 266-67.

471. *See Hearings on H.R. 4077*, *supra* note 48, at 329-30 (statement of Dr. Martin Sepulveda of IBM).

472. *See* Kowalski Testimony, *supra* note 461, at 5.

473. *See id.* at 6. These employers may have a vested interest in minimizing access to identifiable health information; using data in aggregated form may reduce their exposure to employee discrimination lawsuits based on disabilities. *Cf. id.* at 5 (noting that "sound, effective confidentiality policies can help [a] company avoid allegation[s] of discrimination against ill or injured employees"). Of course, if employees are not aware that employers have access to their personal health information, they are not likely to suspect discrimination as a cause for an adverse employment action and are thus less likely to bring a claim under the Americans with Disabilities Act.

staff reveal diagnoses and other treatment information when explaining why employees must miss work or cannot perform certain tasks.[474] Because state confidentiality laws frequently provide weak protection for employee medical records, in-house medical staff often have no legal basis to refuse such demands;[475] those who refuse anyway on ethical grounds are sometimes threatened with dismissal or actually fired.[476] Furthermore, while some contract benefits administrators will not release identifiable claims data on specific employees to self-insured employers,[477] others will do so on demand.[478] The pressure to retain the employer as a customer likely plays a role in their decision to cooperate.[479]

Few legal restrictions currently govern employers' use of employee health data.[480] The 1996 legislative survey of state health confidentiality laws found that only nine states impose a statutory duty of confidentiality on non-health care institutions, including employers.[481] One of these states, California, requires employers to "establish appropriate procedures to ensure the confidentiality and protection" of employees' health information; prohibits the use or disclosure of such information, with some exceptions, without employee authorization; and forbids discrimination against employees who refuse to give authorization.[482] At the federal level,

474. *See id.* at 4.

475. *See Privacy in the Electronic Age Hearings*, *supra* note 75, at 116-17 (prepared statement of the American Association of Occupational Health Nurses).

476. *See id.* at 117; Kowalski Testimony, *supra* note 461, at 4.

477. *See* Larsen Testimony, *supra* note 28, at 15. Mr. Larsen noted, however, that if "push came to shove," the self-insured employer could probably obtain the claims information anyway because "it is really their data. It's their plan." *Id.* at 32.

478. *See* Kathleen Fyffe, Testimony on Behalf of the Health Insurance Association of America Before the Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 34 (Feb. 3, 1997) (unpublished transcript, on file with the *North Carolina Law Review*) [hereinafter Fyffe Testimony].

479. *Cf. Hearings on S. 1360*, *supra* note 54, at 64 (statement of Janlori Goldman, Deputy Director of the Center for Democracy and Technology) ("A few insurers have been candid enough to concede that their primary business relationship is with the employer/customer and not the employee/patient."); Fyffe Testimony, *supra* note 478, at 35 ("It is a challenging relationship [between the employer and the benefits administrator]. The contracts are renewed yearly, and there is quite a bit of competition.").

480. *See Privacy in the Electronic Age Hearings*, *supra* note 75, at 116 (statement of the American Association of Occupational Health Nurses) (noting that state laws frequently provide inadequate protection for employee medical records); *Hearings on S. 1360*, *supra* note 54, at 62 (statement of Janlori Goldman, Deputy Director of the Center for Democracy and Technology) (noting that no federal law prevents self-insured employers from obtaining employees' health data from benefit plans).

481. *See* GOSTIN ET AL., *supra* note 143, at 51.

482. CAL. CIV. CODE § 56.20(a)-(c) (West 1982).

the Americans with Disabilities Act of 1990 ("ADA") forbids discrimination against employees with disabilities[483] but does not address the complete range of health privacy issues at the workplace.[484] Furthermore, as discussed in Part II, courts have expressly recognized, in the absence of contrary law, the right of self-insured employers to monitor their employees' medical claims for the purpose of controlling costs.[485]

Essentially all legislative proposals would apply to employers to the extent that they provide or pay for health care or process health information for their employees.[486] The Administration has, however, adopted the view that employers should be subject to a federal confidentiality law only when serving as a provider or payer and not when processing employee health data obtained through other means.[487] The Administration believes that a "limitation on use" provision—a basic restriction contained in all proposed confidentiality legislation—is sufficient to prohibit self-insured employers from using employee health data for purposes unrelated to payment and to prohibit employers who provide care from using information for purposes other than treatment.[488]

Representatives of the occupational health industry have criticized the Administration's proposal as narrow, arguing that regulating employers only to the extent that they provide or pay for care would not address the full range of situations in which employers might obtain—and misuse—employee health information.[489] In

483. *See* 42 U.S.C. § 12112 (1994).

484. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 15. The ADA's confidentiality provisions apply only to employers with 15 or more employees. *See* 42 U.S.C. §§ 12111(5), 12112(d) (1994). Even when applicable, these provisions offer only limited protection for employees. Employers must treat as confidential all health-related information obtained from medical examinations or medical inquiries as part of an employee health program; this information must be maintained in files separate from regular personnel files. *See id.* § 12112(d)(3)(B). Employers may, however, disclose the information for certain enumerated purposes, including informing supervisors of necessary work accommodations for an employee. *See id.* The statute does not expressly impose a redisclosure prohibition on those who receive this information. *See id.* Furthermore, the confidentiality provisions apply only to information obtained from employees as part of an employee health program at the worksite. *See id.* § 12112(d)(3)(B), (d)(4)(B)-(C). The provisions apparently do not apply to employee health information obtained by other means, such as asking the contract benefits administrator for a list of medications prescribed by an employee's personal physician.

485. *See supra* notes 115-18 and accompanying text (discussing the court's opinion in *Doe v. Southeastern Pennsylvania Transportation Authority*, 72 F.3d 1133 (3d Cir. 1995)).

486. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 15.

487. *See* HHS RECOMMENDATIONS, *supra* note 155, at 20, 26-27.

488. *See id.* at 26-27.

489. *See Privacy in the Electronic Age Hearings*, *supra* note 75, at 118 (prepared

recognition of the serious ramifications of privacy intrusions at the workplace, the NCVHS has also implicitly questioned whether a limitation on use provision is sufficient protection in the employer-employee context; the Committee suggested that all legislation proposed thus far inadequately addresses the range of possible intrusions into employees' privacy.[490] The occupational health industry has concurred with the Committee's assessment by recommending a variety of additional confidentiality safeguards that any federal legislation should incorporate, including a prohibition on coercive practices used to obtain specific employee health information from in-house medical staff.[491]

E. Paper or Computerization?

As discussed in Part II, the use of technology and computerization in health information processing is growing.[492] It is widely acknowledged that computerization poses risks to patients' privacy, enabling large numbers of authorized users to obtain confidential data with ease.[493] Advocacy groups are particularly concerned that patients' computerized records will be linked to massive health databases allowing users from around the nation or world to access these records using a unique patient identifier number.[494] They claim that many of the health confidentiality bills would require patients and providers to switch to computerized information systems and participate in these databases.[495] Because of these concerns, several privacy groups argue that the principle of informed consent requires that patients be allowed to prohibit computerization of their personal information or, at the least, links to shared databases.[496] At least one bill currently before Congress

---

statement of the American Association of Occupational Health Nurses). Other situations in which employers frequently obtain employee health information outside of the treatment or payment process include voluntary wellness programs and mandatory drug tests. *See id.*

490. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 15.

491. *See Privacy in the Electronic Age Hearings*, *supra* note 75, at 125 (prepared statement of the American College of Occupational and Environmental Medicine); *id.* at 120 (prepared statement of the American Association of Occupational Health Nurses).

492. *See supra* notes 51-57 and accompanying text.

493. *See supra* notes 65-70 and accompanying text.

494. *See, e.g.*, *Hearings on S. 1360*, *supra* note 54, at 140 (statement of the Consumer Project on Technology).

495. *See, e.g.*, Breitenstein & Nagel, *supra* note 194, at B6 (referring to "mandatory computerization").

496. *See, e.g.*, *Hearings on S. 1360*, *supra* note 54, at 159 (statement of American Psychiatric Association); Nagel Statement, *supra* note 193, at 2-4; ACLU, *supra* note 251,

would give patients such power, requiring health information trustees to segregate and maintain identifiable information designated by the patient, other than billing data, outside of any computerized networked system.[497]

This approach has been expressly rejected by others. In its report to HHS, the NCVHS concluded that it was "not sympathetic to the notion that patients should have a choice in the technology used to create, store and transmit health information."[498] The Committee explained that Congress had already voiced its approval for the use of computerization to reduce the cost of care[499] and that it would be impractical and burdensome for providers and payers to maintain separately the records of some individuals on paper.[500] It went on to suggest that "[c]omputers are an inevitable part of modern health care .... Patients must accept this and move on to debate the proper protections for records in a computerized environment."[501] The Clinton Administration adopted this view in its recommendations to Congress, adding that giving patients such detailed control over the means by which information flows would actually be harmful because "the effective and rapid processing of information, often for the benefit of the patient, depends on computerized systems."[502]

F. Uniformity and Preemption

In its report to HHS, the NCVHS suggested that the issue of preemption remains "the most difficult conflict" in the health privacy debate.[503] Privacy advocates, patients rights organizations, and physicians groups have argued vigorously that federal law must not preempt state laws that offer more stringent protection or that provide a more expansive right to inspect one's medical records;[504] in other words, federal law should serve merely as a "floor" providing

---

at 1-2.

497. *See* S. 1368, 105th Cong. § 202(f) (1997).

498. NCVHS RECOMMENDATIONS, *supra* note 185, at 10.

499. *See* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C.A. § 1320d, Historical and Revision Notes (West Supp. 1998) (Purpose of Administrative Simplification).

500. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 10.

501. *Id.*

502. HHS RECOMMENDATIONS, *supra* note 155, at 24.

503. NCVHS RECOMMENDATIONS, *supra* note 185, at 16.

504. *See, e.g., Hearings on S. 1360*, *supra* note 54, at 163-64 (statement of the American Psychiatric Association); *id.* at 141-42 (statement of the Consumer Project on Technology); Palmisano Statement, *supra* note 348, at 46.

minimum protection for health information. Advocates are concerned that complete preemption would prevent states from providing additional levels of protection for certain kinds of information, notably that which pertains to HIV status and mental health.[505] AIDS and mental health advocacy groups point to the stigma and discrimination attached to HIV and mental illness and note that unwanted disclosure of information related to these conditions can have potentially dire social and economic consequences.[506] They also assert that strict confidentiality is necessary to encourage those who suffer from these illnesses to seek treatment.[507] The Supreme Court recently added support to this view in *Jaffe v. Redman*.[508] Citing embarrassment caused by unwanted disclosure and noting that "[e]ffective psychotherapy ... depends upon an atmosphere of confidence and trust,"[509] the Court recognized a federal privilege protecting confidential communications between mental health professionals and their patients.[510] Privacy advocates argue that states should be free to respond to concerns such as those cited by the Court by enacting more stringent confidentiality protections than those contained in a federal law.[511]

Insurers, health plans, information processors, and other health care entities with interstate operations have just as clearly indicated that they will only support legislation that offers nearly complete preemption.[512] In their view, any federal law must provide both a "floor" and, to the extent possible, a "ceiling" for confidentiality protection. Legislation that would permit states to create more

505. *See Hearing on S. 1360*, *supra* note 54, at 87-88 (statement of the American Psychological Association); *Hearings on H.R. 4077*, *supra* note 48, at 418 (prepared statement of Aimee R. Berenson of the AIDS Action Council).

506. *See Hearings on S. 1360*, *supra* note 54, at 154-55 (statement of the American Psychiatric Association); Eileen Hansen, Prepared Statement on Behalf of the AIDS Legal Referral Panel Before the Nat'l Comm. on Vital and Health Statistics 1 (June 3, 1997) (unpublished statement, on file with the *North Carolina Law Review*).

507. *See, e.g.*, *Hearings on S. 1360*, *supra* note 54, at 154-55 (statement of the American Psychiatric Association).

508. 518 U.S. 1 (1996).

509. *Id.* at 10.

510. *See id.* at 10-11.

511. *See, e.g.*, *Hearings on S. 1360*, *supra* note 54, at 87-88 (statement of the American Psychological Association); *id.* at 164 (statement of the American Psychiatric Association); *id.* at 101 (statement of the ACLU).

512. *See, e.g.*, *Privacy in the Electronic Age Hearings*, *supra* note 75, at 127 (prepared statement of the Health Insurance Association of America); Letter from James D. Bentley, Senior Vice-President for Policy, American Hospital Association, to John P. Fanning, Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services 1 (July 16, 1997) (on file with the *North Carolina Law Review*); Thompson Statement, *supra* note 54, at 3.

stringent confidentiality laws would offer little, if any, improvement over the existing system of haphazard state laws that inhibit the flow of data.[513]

Health confidentiality bills reflecting the views of both industry and privacy advocates have been introduced in Congress. The Health Care Personal Information Nondisclosure Act of 1998[514] and the Consumer Health and Research Technology Protection Act[515] would preempt state law generally with the exception of laws conferring more stringent protections on public health and mental health information. By contrast, the Medical Information Privacy and Security Act of 1997[516] and the Medical Privacy in the Age of New Technologies Act of 1997[517] have taken the privacy advocates' view that states should be able to enact more stringent confidentiality protections for any kind of health-related information. The Clinton Administration has adopted the privacy advocates' position as well.[518] Explaining its support for more restrictive state laws, the Administration has noted that federal statutes pertaining to privacy rights traditionally preempt only weaker state laws; that states have been careful in their efforts to protect specific classes of information such as HIV and mental health; and that allowing the states to enact more stringent laws would enable the federal government to learn from their experiences.[519] The Administration has not, however, ruled out revisiting the preemption issue at a future date. If permitting states to enact more stringent laws proves confusing to providers or problematic for the health care payment system, it would recommend amending the law to provide more complete preemption.[520]

While reaching consensus on the issue of preemption will not be easy,[521] political realities suggest that it is unlikely a federal law will be enacted without, at the least, preemption exemptions for public and mental health information. Some industry groups have, in fact, conceded this point.[522] It is less likely, however, that a federal law

513. *See, e.g., Hearings on H.R. 4077*, *supra* note 48, at 258-59 (prepared statement of Joel E. Gimpel on behalf of the Workgroup for Electronic Data Interchange).
514. *See* S. 1921, 105th Cong. § 401(a), (c) (1998).
515. *See* H.R. 3900, 105th Cong. § 403(a), (c) (1998).
516. *See* S. 1368, 105th Cong. § 401(a) (1997).
517. *See* H.R. 1815, 105th Cong. § 402(a) (1997).
518. *See* HHS RECOMMENDATIONS, *supra* note 155, at 73-75.
519. *See id.*
520. *See id.* at 17.
521. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 16.
522. *See, e.g., Hearing on S. 1368*, *supra* note 156, at 87 (1998) (statement of the

will incorporate another suggestion made by some privacy advocates—more stringent protections within the federal law for particularly "sensitive" information, notably that related to genetic material and mental health.[523] Users of health care information, as well as many commentators, defend the need for uniformity of protection within the federal law.[524] Instituting multiple levels of protection for different kinds of data, health insurers and commentators respond, will confuse providers and payers and will offer little improvement over the current patchwork of state laws.[525] Because "[c]onfidentiality is in the eye of the beholder," commentators also suggest that it would be presumptuous for Congress to define what is particularly sensitive.[526] An individual with cancer, for example, might consider information pertaining to her illness as sensitive as a patient who is HIV positive, but under the privacy advocates' proposal, the cancer patient might not enjoy the same level of confidentiality.[527] Finally, commentators have expressed concern that treating particular classes of information differently is a slippery slope that would lead to periodic amendment of the federal law to confer more stringent protection on additional conditions.[528] The health care industry instead argues that all health information is sensitive and that a federal law should provide all

---

American Association of Health Plans); NCVHS RECOMMENDATIONS, *supra* note 185, at 16 ("No one has suggested or is likely to support a uniform federal public health law."); Letter from James D. Bentley to John P. Fanning, *supra* note 512, at 1; *The Outcry over HHS's Privacy Proposals*, *supra* note 455, at 8 (discussing the willingness of the Association for Electronic Health Care Transactions to consider a compromise on the issue of preemption of public health and mental health laws).

523. *See, e.g.*, *Hearings on S. 1360*, *supra* note 54, at 88 (statement of the American Psychological Association); NCHVS RECOMMENDATIONS, *supra* note 185, at 17. For additional discussion of why mental health information deserves special protection, see Elaine Brooks et al., *Confidentiality and Right to Privacy Issues in Mental Health Managed Care*, 19 WHITTIER L. REV. 39 (1997).

524. *See, e.g.*, *Privacy in the Electronic Age Hearings*, *supra* note 75, at 128 (prepared statement of the Health Insurance Association of America); GOSTIN ET AL., *supra* note 143, at 43, 156; LOWRANCE, *supra* note 66, at 16-17.

525. *See, e.g.*, *Hearings on H.R. 52*, *supra* note 27, at 75 (statement of Merida L. Johns, President of the American Health Information Management Association) (suggesting that special precautions for certain kinds of information will confuse providers); *Privacy in the Electronic Age Hearings*, *supra* note 75, at 94 (statement of John T. Nielsen on behalf of the American Association of Health Plans) (arguing that multiple levels of protection will not improve the current situation).

526. Gellman Statement, *supra* note 446, at 63.

527. *See, e.g.*, GOSTIN ET AL., *supra* note 143, at 156.

528. One observer has described this concern as the "disease of the month phenomenon." Robert Gellman, Chairman Statement, Subcomm. on Privacy and Confidentiality of the Nat'l Comm. on Vital and Health Statistics 53 (Jan. 13, 1997) (unpublished transcript, on file with the *North Carolina Law Review*).

information with the same level of strong protection.[529] Thus far, many of the comprehensive proposals introduced in Congress have adopted the industry's view on the uniformity issue.[530]

V. CONCLUSION

The foregoing analysis reveals that while there are many areas of agreement concerning privacy protections for health records, there remain as many points of disagreement. These differences reflect the inherent tension in the relationship between the individual's right to privacy and society's interest in high quality, cost-effective health care.[531] As this tension cannot be resolved completely in favor of one interest or another, a balance must be struck that respects the compelling claims of both interests. Reaching this balance necessarily requires some amount of compromise by all parties[532]—especially in the following areas—so that meaningful privacy protections can be enacted into law before the HIPAA deadline expires.

First, law enforcement must accept new restrictions on its ability to access individually identifiable health information. At the federal level, where most investigation into health fraud occurs, there is little oversight of law enforcement's ability to obtain such information;[533] the same is true in some states.[534] The Clinton Administration's proposal would not substantially change existing practice.[535] Secretary Shalala has stated that no one should have a "free pass" to obtain information,[536] but in many cases, law enforcement effectively has such a pass.[537] Although law enforcement often has a compelling

529. *See Hearings on H.R. 52*, *supra* note 27, at 102-03 (statement of Sherine Gabriel on Behalf of the Healthcare Leadership Council).

530. *See* S. 1921, 105th Cong. (1998); H.R. 3900, 105th Cong. (1998); H.R. 52, 105th Cong. (1997); S. 1360, 104th Cong. (1995). *But see* S. 1368, 105th Cong. § 202(f) (1997) (permitting an individual to require a health care information trustee to segregate certain health information and to adhere to more stringent confidentiality practices); H.R. 3482, 104th Cong. § 201(c) (1996) (same).

531. *See supra* notes 190-201 and accompanying text.

532. *See* GOSTIN ET AL., *supra* note 143, at 12 (arguing that "[a]bsolutist positions ... will not result in health information systems that can effectively serve" the dual goals of providing good health care and protecting patient's privacy); NCVHS RECOMMENDATIONS, *supra* note 185, at 4 ("None of these benefits will be achieved unless everyone approaches the legislative process with a spirit of compromise.").

533. *See supra* notes 420-28 and accompanying text.

534. *See supra* text accompanying note 419.

535. *See supra* notes 449-54 and accompanying text.

536. *Privacy in the Electronic Age Hearings*, *supra* note 75, at 24 (prepared statement of Donna Shalala, Secretary of HHS).

537. *See supra* notes 420-28 and accompanying text.

need to obtain health data, the sensitive nature of this information and the ramifications of its use are of such import that agencies should always have to demonstrate this need to a court before accessing records. Law enforcement officials claim that such a requirement would be unduly burdensome,[538] but tightened restrictions are not without precedent. Federal law already requires law enforcement agencies to obtain a court order before accessing personally identifiable information concerning cable television subscriptions;[539] officials must establish by clear and convincing evidence that the information sought is material to the present investigation.[540] Our health-related information, undoubtedly as sensitive, surely deserves as much protection.

Second, privacy advocates must acknowledge the presence and benefits of technology in health information processing. The confidentiality debate has frequently dwelled on the risks posed by computerization at the expense of recognizing its benefits.[541] While these risks are real and must be addressed in the legislation, they should not blind us to the potential gains in both quality and efficiency of care. Rather than fight the use of new information technologies in health care, privacy advocates should accept their presence and expend their energy assisting in the creation and enforcement of clear and meaningful guidelines governing the use and disclosure of information.[542] It would be both unrealistic and a waste of limited resources to require those who use health information to create two systems, computerized and paper-based, for its storage and transfer.[543] The right to privacy is compelling but not absolute and cannot be permitted to disrupt the entire health care treatment and payment system. As one commentator has observed, "[i]ndividuals already forego significant levels of privacy in order to obtain the social goods that benefit society collectively," and while not every person is satisfied with this "social contract ... all individuals benefit."[544] For this reason, he has noted, "[a] complex modern society cannot elevate each person's interest in privacy above other important societal interests."[545]

538. *See supra* notes 440-48 and accompanying text.
539. *See* 47 U.S.C. § 551(h) (1994).
540. *See id.*
541. The NCVHS reached the same conclusion in its report. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 6.
542. *See id.* at 10.
543. *See id.*
544. Gostin, *supra* note 12, at 515.
545. *Id.*

Third, given the increasingly integrated nature of the health care industry and its growing reliance on computerized patient records and electronic claims processing, uniformity in protection and substantial preemption of state law are necessary.[546] Incorporating more stringent privacy protections within the federal law for information some deem particularly "sensitive," notably that related to genetic material and mental illness, would undermine one of the fundamental reasons for enacting a federal law and would result in additional administrative burdens, confusion, and possibly inadvertent violations.[547] Similarly, permitting states to enact more restrictive confidentiality provisions for any kind of health information would offer little, if any, improvement over the status quo, which requires payment and treatment entities to attempt to comply with as many as fifty sets of laws.

At the same time, however, users of health information cannot realistically expect complete preemption. First, in deference to the states' longstanding role as guardians of the public health, a federal confidentiality law should not preempt state reporting laws or more stringent public health laws. Public health agencies have established an admirable record of protecting individuals' confidentiality while operating under laws particular to each state.[548] These laws function well and have the support of the state agencies; to preempt those that are more stringent would only cause confusion among public health officials.[549] Second, in deference to the fast-approaching HIPAA deadline, the health care industry should accept the possibility of stronger state laws regarding the confidentiality of mental health information. Given the strong opposition to total preemption by the mental health community, as well as the Supreme Court's recent recognition of the sensitivity of such information, preemption of stronger state laws in this area may be politically unrealistic. Incorporating these two limited exceptions to preemption strikes a reasonable balance between the need for substantial uniformity on one hand, and respect for the functions of state government and awareness of the need to pass confidentiality legislation in a timely manner, on the other.[550]

546. *See supra* notes 27, 161-70 and accompanying text.

547. *See supra* notes 169, 524-25 and accompanying text.

548. *See supra* note 383 and accompanying text.

549. *See supra* notes 384-85 and accompanying text.

550. As previously noted, some users of health care information understand the need for compromise in these areas and have expressed a willingness to accept federal legislation permitting more stringent public health and mental health confidentiality laws at the state level. *See supra* notes 521-22 and accompanying text.

Any meaningful federal health confidentiality law must also include express restrictions on employers' ability to access employees' health information. While the ADA provides a measure of protection for some employees, it does not address the full spectrum of potential privacy violations in the workplace.[551] Furthermore, although current legislative proposals would limit the use of data by any trustee to the purpose for which it was collected,[552] the potential consequences of an employer learning unfavorable information about an employee are so serious that a more definitive wall between personal health information and employment should be constructed. At the least, employers should not be allowed to coerce in-house medical staff into disclosing specific health-related information about employees, and self-insured employers should not be permitted to obtain individually identifiable treatment and prescription information about their employees from their benefit plan administrators.[553] While employers have a legitimate need to regulate expenses and to ensure workplace safety, the experience of companies with voluntary restrictions demonstrates that they can do so using non-identifiable or only generalized information.[554]

Many other areas, of course, require compromise. Unfortunately, if the past is any indication, it is by no means certain that compromise will be forthcoming. Eighteen years have passed since the 96th Congress considered the first comprehensive legislation, yet we are still without uniform privacy protection for our most sensitive information.[555] While genuine support exists for a federal law, many parties have been unwilling to make the concessions necessary to accomplish this goal.[556] Observers are split as to whether the 105th Congress will distinguish itself in this regard.[557] If it does not, there is a substantial likelihood that much of

551. *See supra* notes 483-84 and accompanying text.

552. *See supra* note 488 and accompanying text.

553. *Cf.* Letter from James D. Bentley to John P. Fanning, *supra* note 512, at 2 (expressing the American Hospital Association's view that self-insured employers should be covered by federal confidentiality legislation).

554. *See supra* notes 467-73 and accompanying text.

555. *See supra* notes 76-78 and accompanying text.

556. The NCVHS noted, for example, that while users of health information professed support for patient privacy, they did not want restrictions on their ability to use or obtain data. *See* NCVHS RECOMMENDATIONS, *supra* note 185, at 3. The Committee found this position "unreasonable." *Id.* Responding to arguments by privacy advocates, the Committee also noted that "no one can expect that the health care system will be restructured solely in the interests of privacy." *Id.*

557. Privacy consultant Robert Gellman does not believe the 105th Congress will pass a bill, but Thomas Gilligan, a lobbyist for the health information processing industry, has

our sensitive health information will be left to the protection of regulations alone.[558]

BARTLEY L. BAREFOOT

estimated the odds at 60-40 that a bill will pass. *See The Outcry over HHS's Privacy Proposals*, *supra* note 455, at 8.

558. *See supra* notes 233-36 and accompanying text.