


1999

Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age"

Patricia I. Carter

Follow this and additional works at: <http://open.mitchellhamline.edu/wmlr>

Recommended Citation

Carter, Patricia I. (1999) "Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age" , " *William Mitchell Law Review*: Vol. 25: Iss. 1, Article 1.

Available at: <http://open.mitchellhamline.edu/wmlr/vol25/iss1/1>

This Article is brought to you for free and open access by the Law Reviews and Journals at Mitchell Hamline Open Access. It has been accepted for inclusion in William Mitchell Law Review by an authorized administrator of Mitchell Hamline Open Access. For more information, please contact sean.felhofer@mitchellhamline.edu.

© Mitchell Hamline School of Law

HEALTH INFORMATION PRIVACY: CAN CONGRESS PROTECT CONFIDENTIAL MEDICAL INFORMATION IN THE “INFORMATION AGE”?

Patricia I. Carter[†]

“Right now, the way we currently protect the privacy of our medical records is erratic at best—dangerous at worst. It is time for our nation to enact federal legislation to protect the age-old right to privacy in this new world of progress.”[†]

I. INTRODUCTION	225
II. THE COMPUTERIZATION OF MEDICAL RECORDS AND OTHER HEALTH CARE INFORMATION	226
III. BALANCING THE BENEFITS AND RISKS OF SHARING HEALTH CARE DATA	231
A. <i>The Importance of Confidentiality</i>	231
B. <i>The Need to Share Medical Data</i>	232
C. <i>The Risk of Disclosure</i>	233
IV. COMPUTER DATA SECURITY	234
V. ETHICAL PROTECTION OF THE RIGHT TO PRIVACY	236
VI. FEDERAL LEGAL PROTECTIONS	238
A. <i>Constitutional Right to Privacy</i>	238
B. <i>Federal Legislation</i>	241
1. <i>The Privacy Act of 1974</i>	241

† The author is an associate at Gray, Plant, Mooty, Mooty & Bennett, P.A., in Minneapolis, where she practices in the area of health and human services law. Ms. Carter is a *magna cum laude* graduate of Hamline University School of Law. Formerly, Ms. Carter was a manager and consultant in the field of health claims information systems.

1. CONFIDENTIALITY OF INDIVIDUALLY-IDENTIFIABLE HEALTH INFORMATION: RECOMMENDATIONS OF THE SECRETARY OF HEALTH & HUMAN SERVICES, PURSUANT TO SECTION 264 OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, submitted to the Senate Comm. on Labor & Human Resources, the Senate Comm. on Finance, the House Comm. on Commerce, and the House Comm. on Ways & Means, § I (Sept. 11, 1997) <<http://aspe.os.dhhs.gov/admnsimp/vpcrec0.htm>> [hereinafter SHALALA REPORT].

	2. <i>Freedom of Information Act (FOIA)</i>	244
	3. <i>Other Federal Legislation</i>	245
VII.	STATE LEGAL PROTECTIONS	245
	A. <i>Categories of State Privacy Protections</i>	246
	1. <i>State Constitutional Protections</i>	246
	2. <i>State Common Law</i>	247
	3. <i>State Legislation</i>	249
	4. <i>Exceptions to Confidentiality Regulation</i>	251
	B. <i>Uniform Health-Care Information Act</i>	252
	C. <i>State Privacy Laws: California, Tennessee and Minnesota</i>	253
	1. <i>Privacy in California</i>	254
	2. <i>Privacy in Tennessee</i>	258
	3. <i>Privacy in Minnesota</i>	260
VIII.	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)	266
IX.	PROPOSED FEDERAL PRIVACY LEGISLATION	268
	A. <i>Recommendations of the Secretary of Health & Human Services</i>	271
	B. <i>Current Issues in Legislating Health Information Privacy</i>	272
	1. <i>Balancing Private Rights and Public Purposes</i>	272
	2. <i>Scope of Action</i>	272
	3. <i>Patient Access to Records</i>	274
	4. <i>Informed Consent</i>	276
	5. <i>Disclosures for Public Purposes</i>	278
	a. <i>Oversight of the Health Care System</i>	278
	b. <i>Public Health</i>	279
	c. <i>Medical Research</i>	279
	d. <i>Law Enforcement</i>	282
	6. <i>Penalties/Sanctions</i>	283
	7. <i>Federal Pre-emption</i>	283
	8. <i>Summary</i>	285
X.	CONCLUSION.....	285

I. INTRODUCTION

As we use the health care system, personal medical data² is collected, stored and disseminated. Most of us no longer have a family doctor who protects this information in a locked file cabinet in her office. In this "information age," this very personal information is now in electronic form and is exchanged easily among health providers, insurance companies and others in the modern health care delivery system.

Automated medical data systems have led to both great potential benefits and increasing confidentiality concerns. Computerization offers opportunities to improve health care delivery and administration, and to provide valuable research and public health information. However, it also means that this information is no longer as easily protected, and at the same time, the number of individuals and organizations with access is expanding. Health care information is communicated to other health care providers, billing services, third-party payors, research organizations, and public health agencies. While technology can provide some answers with respect to data security, this is not only a technical problem but a procedural, ethical and legal one.

This article will first examine advances in computer and communication technology, and the subsequent affect on health information privacy issues,³ including the balancing of the benefits and risks of sharing health care data. A brief discussion of com-

2. The terms "medical data," "medical information," "health care data," and "health care information" are used interchangeably in this article to refer to a broad range of information collected in the course of an individual's experiences with the health care delivery system. "Medical record" or "patient record" is used more narrowly to describe a record generated and maintained by a health care provider in the course of delivery of health care, and containing information which can be readily matched to an individual.

3. While some commentators distinguish between confidentiality and privacy, in this article the terms will be used interchangeably. See U.S. CONG., OFFICE OF TECHNOLOGY ASSESSMENT, PROTECTING PRIVACY IN COMPUTERIZED MEDICAL INFORMATION, OTA-TCT-576, at 7-9 (1993) [hereinafter PROTECTING PRIVACY]. For example, PROTECTING PRIVACY cites Alan Westin's view that "privacy" is the claim of an individual to decide when, how and to what extent information about themselves is communicated to others. See *id.* at 8. Privacy balances the needs of society for the information and the individual's control over disclosure. See *id.* Whereas, "confidentiality" refers to how data collected for approved purposes is maintained and used by the organization that collected it, and what secondary uses may be made of it, and when the individual's consent is required for such secondary uses. See *id.* at 9.

puter security issues is provided, but because a completely secure system is impossible, the main focus of this article will be on the legal protections available for this information. This article will review the various sources of legal rights to confidentiality of individual health care information and will conclude that the current complex patchwork of federal and state protections is insufficient in this age of information technology. Comprehensive federal legislation will be required to meet the challenge of maintaining the confidentiality of individually-identifiable medical information, while still making appropriate information available for necessary and valuable public uses. This article will then present and evaluate current proposals for meeting this challenge.

II. THE COMPUTERIZATION OF MEDICAL RECORDS AND OTHER HEALTH CARE INFORMATION

Computer technology is transforming the way medical records are maintained and the way health care information is shared. Initially, computerized systems for patient information were primarily associated with large hospitals and clinics, allowing health care providers and administrators within the institution to access the information.⁴ Advances in technology, including network communications, relational databases, advanced database retrieval tools, and increased speed and storage capacity, have made it possible to collect, store and retrieve large amounts of health care data, and to disseminate that data across sophisticated communication networks.

Telemedicine combines the advances of telecommunications and health care.⁵ Telemedicine encompasses a variety of methods, but all include "some remote interaction between a physician and a patient, whether by facsimile, telephone, satellite or fiber-optic cable."⁶ Telemedicine is seen as having great potential for providing much needed health care in rural areas where there are few physi-

4. *See id.* at 6, 8.

5. *See generally* Symposium, *1997 Telemedicine Symposium*, 73 N.D. L. REV. 1 (1997) (containing nine articles discussing various aspects of telemedicine). The symposium authors addressed a number of critical issues in the ongoing development of telemedicine including its role in health care delivery, impact on licensure, related medical malpractice issues, evolution of network infrastructures, and some possible solutions. *See generally id.*

6. Kerry A. Kearney, *Medical Licensure: An Impediment to Interstate Telemedicine*, 9:4 HEALTH LAW., 1997, at 14, 14.

cians.⁷ As telemedicine develops, increasing amounts of medical data will be transmitted electronically.

Health care claims information is increasingly being transferred electronically from providers to third-party payors. The federal government has led the way in computerization of claims information. The Workgroup for Electronic Data Interchange (WEDI) was established by the Department of Health and Human Services in 1991 to promote electronic claims submission.⁸ The Health Care Financing Administration (HCFA), which administers Medicare claims through contracts with private insurance carriers, promoted electronic claims submission by requiring those carriers to reimburse providers more quickly if they submitted their claims electronically.⁹ Now seventy-nine percent of all Medicare claims are processed electronically (including nearly seventy-one percent of Part B claims).¹⁰ Private payors are not far behind. The nation's

7. See Paul M. Orbuch, *A Western States' Effort to Address Telemedicine Policy Barriers*, 73 N.D. L. REV. 35, 35 (1997). For example, a computer-linked interactive video system would allow an urban specialist to examine a patient at a rural clinic in consultation with the on-site rural physician. See *id.* at 35-36. A simpler example would be if the rural physician sent x-rays by facsimile to a radiologist for review. See *id.* at 36.

8. See U.S. GENERAL ACCOUNTING OFFICE, *MEDICARE: ANTIFRAUD TECHNOLOGY OFFERS SIGNIFICANT OPPORTUNITY TO REDUCE HEALTH CARE FRAUD*, GAO/AIMD 95-77 (Aug. 11, 1995), available in GAO-RPTS, 1995 WL 579415 (letter report to the ranking minority member of the Subcomm. on Labor, Health and Human Servs., and Educ. of the Senate Comm. on Appropriations).

9. See *id.* at 12. Paper claims were reimbursed in 27 days; electronic claims in 14 days. See *id.* HCFA was to require all hospital claims to be submitted electronically by 1999 in order to facilitate the detection of claims fraud and abuse. See Medicare Program: Uniform Hospital Billing and Payment Mechanisms, 58 Fed. Reg. 4705, 4705 (1993) (proposed rule); see also Edward L. Schrenk & Jonathan B. Palmquist, *Fraud and Its Effects on the Insurance Industry*, 64 DEF. COUNS. J. 23, 26 (1997) (analyzing the growing problem of insurance fraud and recommending strategies to combat the problem). However, plans for the national Medicare payment computer system, which was to enable HCFA to fight Medicare fraud more effectively, were halted. See Robert Pear, *Medicare Overhaul is Halted*, N.Y. TIMES, Sept. 16, 1997, at A4; *Clinton Cancels Plans to Modernize Medicare Reimbursement System*, MEALEY'S LITIG. REP. INS. FRAUD, Sept. 25, 1997, available in WESTLAW, 4:16 MLRINSF 5 [hereinafter MEALEY'S]. The project had begun in 1994 and had cost \$102 million through September, 1996. See MEALEY'S, *supra*, at 5. The project turned out to be "far more complicated" than federal officials had anticipated. *Id.*

10. See Howard Larkin, *Medicare Shapes Up Claims*, AM. MED. NEWS, Aug. 26, 1996, at 21. Medicare claims are divided into two parts: Part A includes inpatient hospital, skilled nursing facility, hospice, and some home health care services; Part B includes physician services, outpatient hospital services, diagnostic tests, ambulance and other medical services and supplies. See U.S. GENERAL ACCOUNTING OFFICE, *MEDICARE: HCFA FACES MULTIPLE CHALLENGES TO PREPARE FOR THE 21ST*

Blue Cross/Blue Shield plans electronically process sixty-six percent of claims.¹¹ Other commercial carriers electronically process twenty percent of claims.¹² Most physicians, however, still submit claims by sending paper through the mail.¹³ But this is changing. New Internet services are springing up, allowing even small physician offices to file claims electronically.¹⁴

The Internet is also being explored as a means of accessing patient medical records. The University of California San Diego School of Medicine has announced a ground-breaking project that will put full medical records on the Internet.¹⁵ The Patient Centered Access to Secure Systems Online (PCASSO) is intended to provide patients with access to their own records and to allow their physicians to retrieve patient records from any computer with Internet access.¹⁶

This movement toward electronic data interchange (EDI) will be accelerated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).¹⁷ HIPAA mandates that certain key players in the health care system, such as insurers, have the capability to handle electronic transactions by the year 2000.¹⁸ Some commentators have expressed concerns that HIPAA will lead us down the road to electronic health care data before there are sufficient privacy safeguards in place;¹⁹ however, the health care industry is already maintaining and disseminating health care information electronically, on an ever-increasing scale.²⁰

CENTURY 2, GAO/T-HEHS-98-85 (Jan. 29, 1998) (reporting testimony of William J. Scanlon, Director of Health Financing and Systems Issues, before the Subcomm. on Health of the House Comm. on Ways & Means).

11. See Larkin, *supra* note 10, at 21.

12. See *id.*

13. See Greg Borzo, *Claims Stake a Claim on the Internet*, AM. MED. NEWS, Aug. 11, 1997, at 21.

14. See *id.* See generally *Claimsnet* (visited Jan. 18, 1999) <<http://www.claimsnet.com/public>> (providing Internet claims submission services for physicians).

15. See Greg Borzo, *PCASSO With a Mouse*, AM. MED. NEWS, Oct. 13, 1997, at 24. The first 250 patients, all volunteers, were to have their medical records put on the Internet in January 1998 for an initial test. See *id.*

16. See *id.*

17. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C. and 42 U.S.C.) (also referred to as the Kassebaum-Kennedy Act). See *infra* Part VIII for a discussion of this legislation.

18. See 42 U.S.C. § 1320d-2, -4 (1997); see *infra* Part VIII.

19. See *infra* note 290 and accompanying text.

20. Other examples of the collection and maintenance of electronic health care data include the Medical Information Bureau (MIB), a computerized service

Medical information is rarely restricted to the state in which it originated.²¹ Health care information is routinely transmitted to other states, for purposes of claims payment, utilization review, public health purposes, and medical research.²² This information then becomes subject to a wide range of privacy protections, which are only as predictable as the ultimate destination of that information.²³ Furthermore, with the advance of computers and telecommunications, physical location of the data becomes less and less relevant.²⁴ Remote access to a database becomes as simple as local

that maintains data on the health histories of millions of Americans. See JO ANNE CZECOWSKI BRUCE, *PRIVACY AND CONFIDENTIALITY OF HEALTH CARE INFORMATION* 113 (2d ed. 1988). Subscribing insurance companies contribute data on their own insured populations, and they can retrieve data on other individuals on request. See *id.* This information can then be used to evaluate insurance applications and for other purposes. See *id.* Public health agencies collect, store and use vast amounts of medical information. See Lawrence O. Gostin et al., *Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization*, pt. 4, § II.A. (Feb. 1997) (visited Jan. 18, 1999) <http://www.epic.org/privacy/medical/cdc_survey.html>. This information is used to identify and control communicable diseases, study environmental risks, and the effects of behaviors on health. See *id.* "The development of a public health information infrastructure is . . . an emerging reality. National, regional and statewide databases are rapidly becoming repositories of a vast amount of public health information." *Id.* Numerous databases maintain comprehensive data on population-based research, and data registries are maintained for specific diseases (such as AIDS). See *id.* The success of public health efforts in the areas of disease surveillance and epidemiological research depend on the information technology. See *id.* Public health agencies have been very good at preventing unauthorized disclosures of personally-identifiable health data, but concerns remain about the government holding this personal data. See *id.* pt. 4, § II.B. Gostin believes these concerns are justified, and that "significant levels of privacy cannot exist within the government's wide and complex web of data collection." *Id.*

Fully electronic medical records systems are still the exception, because of high costs and uncertain benefits. See Allan Khoury, *Finding Value in EMRs (Electronic Medical Records)*, HEALTH MGMT. TECH., July 1997, at 34. See generally THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE (Richard S. Dick & Elaine B. Steen eds., 1991) (finding that, while most industries were moving to computerized data, medical records were still being kept on paper, and providing guidance for creating computer-based patient records (CPR)). Nevertheless, the number of successful EMR implementations is now growing. See Khoury, *supra*, at 34. For instance, Kaiser Permanente of Ohio, a large health maintenance organization (HMO), began development of its EMR system in 1989; today the system is fully implemented. See *id.* Kaiser planned to phase out the delivery of paper charts starting in September 1997. See *id.*

21. See Lawrence O. Gostin et al., *Privacy and Security of Personal Information in a New Health Care System*, 270 JAMA 2487, 2489-90 (1993).

22. See *id.* at 2490.

23. See *id.*

24. See *id.*

access. Attempts to regulate the privacy of information based on the physical location of the data ignore the realities of the computer age.²⁵

This increase in the use of computers in health care raises concerns because of the apparent ease with which vast amounts of information can be accessed and aggregated. The public's twofold distrust of technology and bureaucracy causes individuals to be concerned that unauthorized persons will be able to gain access to their personal information.²⁶ There are those who now believe that "the only reasonable expectation of privacy is no expectation of privacy at all."²⁷

While it may be premature to proclaim the demise of privacy, it is certain that "the exponential increase in the use of computers and automated information systems for health-record information . . . [has contributed to the] substantial pressure on traditional confidentiality protections."²⁸ As a result of advances in computer and communications technology, and the linking of computer networks, patient information will no longer be confined to a single institution. Indeed, health care data may originate in a combination of facilities, and be maintained and accessed across great distances. This places a strain on the protections of health care data currently in place:²⁹

Existing models for data protection, which place responsibility for privacy on individual . . . [health care providers], will no longer be workable for new systems of computer linkage and exchange of information across high performance, interactive networks. New approaches to data protection must track the flow of the data itself.³⁰

25. *See id.*

26. *See* Gostin et al., *supra* note 20, pt. 4, § VI.B.

27. Scott Burris, *Healthcare Privacy & Confidentiality: The Complete Legal Guide*, 16 J. LEGAL MED. 447, 451 (1995) (reviewing JONATHAN P. TOMES, *HEALTHCARE PRIVACY & CONFIDENTIALITY: THE COMPLETE LEGAL GUIDE* (1994)). "Privacy doctrine today is largely devoted to perpetuating a myth—a myth of 'privacy rights' in which autonomous individuals are capable of exercising actual control over information that is to be found in the minds or papers of identifiable individuals." *Id.*

28. UNIF. HEALTH-CARE INFORMATION ACT, prefatory note, 9 pt. I U.L.A. 475 (1988).

29. *See* PROTECTING PRIVACY, *supra* note 3, at 9.

30. *Id.* at 9-10.

III. BALANCING THE BENEFITS AND RISKS OF SHARING HEALTH CARE DATA

A. *The Importance of Confidentiality*

The confidentiality of personal information is increasingly a matter of public concern.³¹ Public opinion polls consistently find that Americans are very concerned about protecting the confidentiality of personal medical data and support government regulation to protect that information.³²

The intimate character of personally-identifiable medical information raises a number of concerns. First, patients are often both physically and mentally vulnerable at the time of treatment; this weakened condition should compel special protections.³³ Second, patient autonomy is the basis for current theoretical justifications for a right of privacy.³⁴ This "autonomy encompasses the right to control the dissemination of personal health information."³⁵ Third, trust is essential to the physician-patient relationship, and this trust depends on the patient's belief that the physician will

31. See U.S. CONG., OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC RECORD SYSTEMS AND INDIVIDUAL PRIVACY, OTA-CIT-296, at 13 (1986). This federal agency report concluded that privacy is a significant and enduring value held by Americans. See *id.*

32. In January 1998, a *Los Angeles Times* poll found that 88% of respondents supported a consumer bill of rights for health maintenance organizations (HMO) that would guarantee that medical records be kept confidential. See L.A. TIMES Poll, Feb. 2, 1998, at A1. This consumer bill was one of the proposals presented by President Clinton in his State of the Union Address, January 27, 1998. See *id.* The question asking about support for the consumer bill also indicated that the bill would guarantee that medical decisions were made by medical doctors. See *id.* This may have influenced the respondents' answers. However, other polls have found similar results. A 1993 Harris poll found that 97% of respondents believed in the importance of protecting the confidentiality of individual's medical records, with 36% classifying such protection as "absolutely essential." Louis Harris & Assoc. Poll, Nov. 1993, available in WESTLAW, POLL database, File USHARRIS.93PRIV RC01C. See also Lawrence O. Gostin et al., *Privacy and Security of Health Information in the Emerging Health Care System*, 5 HEALTH MATRIX 1, 2 (1995) (citing LOUIS HARRIS & ASSOCS., HEALTH INFORMATION PRIVACY SURVEY 22 (1993), which found 78% of respondents expressed concern that their privacy rights were not adequately protected, and 80% of respondents believed consumers have "lost all control over how personal information about them is circulated and used"). Polls also show that 96% of Americans believe that rules should be spelled out as to who has access to medical records and what information can be obtained. See Louis Harris & Assoc. Poll, Nov. 5, 1993, available in WESTLAW, POLL database, File USHARRIS.110593 R3A.

33. See Gostin et al., *supra* note 20, pt. 2, § III.

34. See *id.*

35. *Id.*

maintain the confidentiality of the patient's disclosures.³⁶ Fourth, candor in the physician-patient relationship is dependent on the expectation of confidentiality. Failure to respect informational privacy may cause patients to withhold information vital to their care or to be reluctant to seek care altogether.³⁷ Finally, "unauthorized disclosure of information could result in embarrassment, stigma, and discrimination."³⁸

B. *The Need to Share Medical Data*

Patients cannot have absolute control over their medical information because access to this data is essential for the modern provision of health care. Patient data is commonly shared with other health care providers, insurance companies, utilization review services, preferred provider organizations, and health maintenance organizations. This sharing of information is required for the functioning of the health care system. When a patient is transferred or referred to another health care provider, or under other compelling circumstances affecting the patient's health, patient medical records should be immediately available.³⁹ Accurate and complete health care information is critical to the physician-patient relationship, and to the provision of quality care. The computerization of patient records can improve patient care by providing more complete, accurate and timely information.⁴⁰ Patient records can be transmitted from one health care facility or provider to another, to improve the integration of services. Computerization can also improve retrieval time for patient records and prevent the misuse and misplacement of medical data.⁴¹

Computerized health care data also has the potential to contribute to medical research⁴² and to enhance capabilities for making resource allocation and utilization management decisions.⁴³ Furthermore, the electronic data interchange of health care infor-

36. *See id.*

37. *See id.*

38. *Id.*

39. BRUCE, *supra* note 20, at 110.

40. *See* WILLIAM H. ROACH, JR. ET AL., *MEDICAL RECORDS AND THE LAW* 155 (2d ed. 1994).

41. *See id.* at 155-56.

42. *See* PROTECTING PRIVACY, *supra* note 3, at 8-9 (citing INSTITUTE OF MEDICINE, *THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE* (Richard S. Dick & Elaine B. Steen eds., 1991)).

43. *See id.*

mation could create substantial economic savings and reduce time-consuming paperwork burdens.⁴⁴

The administration of our health care system depends on the flow of information. When pre-approval is required for a medical procedure, patients must authorize release of their medical records to obtain that approval. Prior to payment being made, medical data must be released to insurance companies and other third-party payors. There are so many legitimate groups with legitimate reasons for accessing medical information that it is very difficult to prevent its spread and impossible to even identify all these groups.⁴⁵ Thus, the issue of privacy of health data becomes a matter of controlling *authorized* access to information.

C. *The Risk of Disclosure*

A 1994 report by the Institute of Medicine identified three common types of disclosure that pose a threat to medical data privacy.⁴⁶ First is the inadvertent disclosure that may occur unthinkingly within medical institutions.⁴⁷ These disclosures include information left displayed on a computer screen and conversations about confidential patient information held in common areas or over cellular phones.⁴⁸ These types of disclosures can be handled through internal policies and procedures within the institution.⁴⁹ The second type of disclosure is the “routine” release of information. Health information is often shared without the specific knowledge of the patient, based on a blanket consent.⁵⁰ Such blanket consent may be obtained from a patient prior to receiving care or upon enrolling in a health insurance plan.⁵¹ The Institute of Medicine report found protection against this type of disclosure to be in need of strengthening.⁵² The third and final type of disclosure is secondary use—the re-release of information to third parties

44. *See id.*

45. *See* INSTITUTE OF MEDICINE, HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY 151-52 (Molla S. Donaldson & Kathleen N. Lohr eds., 1994) [hereinafter Donaldson & Lohr].

46. *See id.* at 157-60.

47. *See id.*

48. *See id.*

49. *See id.*

50. *See id.* at 158.

51. *See id.*

52. *See id.*

without the subject's knowledge or consent.⁵³ The control of secondary use is an important principle of data privacy. Information that is collected for a particular purpose should be used only for that purpose.⁵⁴ This is the most difficult type of disclosure to control. Examples include the sharing of information between different departments within an insurance company or health maintenance organization (HMO), or between a health provider and an employer, and insurance companies sharing information through the Medical Information Bureau.⁵⁵ This type of disclosure to third, fourth or fifth parties is arguably most in need of additional controls.

A balance must be struck between the public benefits of making health information available and individual expectations of privacy in that information. While it may not be possible to strike a perfect balance, these competing interests must be addressed. One important consideration is whether the medical data is individually-identifiable; that is, can the medical information be easily linked to the individual patient.⁵⁶ This type of information is in need of the highest degree of protection. Wherever possible, the patient's consent should be obtained prior to disclosure of individually-identifiable medical data, even if the disclosure is for a legitimate purpose.⁵⁷

IV. COMPUTER DATA SECURITY

The collection and distribution of larger and larger amounts of health care data through automation raises concerns about both data security and confidentiality.⁵⁸ Data security refers to the tech-

53. *See id.*

54. *See* The Privacy Act, 5 U.S.C. § 552a(b) (1994). The federal Privacy Act reflects this principle by permitting nonconsensual secondary uses of personal data only for purposes that are consistent with the purpose for which data were first collected. *See id.*

55. *See* Donaldson & Lohr, *supra* note 45, at 158.

56. *See* Gostin et al., *supra* note 20, pt. 4, § II.B.

57. *See id.* pt. 4, § III.

58. *See* U.S. CONG., OFFICE OF TECHNOLOGY ASSESSMENT, DEFENDING SECRETS, SHARING DATA: NEW LOCKS AND KEYS FOR ELECTRONIC INFORMATION, OTA-CIT-310 (1987). This 1987 federal agency report examined the vulnerability of data and communications systems, and the technology available to safeguard data. *See id.* At that time, government agencies, the private sector and individuals were already using sophisticated computer and communication technologies to acquire, store, process, and disseminate information that needed to be protected. *See id.* In the decade since this report, technological capabilities have advanced exponentially,

nical and procedural mechanisms used to assure that only authorized persons have access to the data;⁵⁹ whereas, confidentiality refers to the policy and legal determinations of who should have access to that data.⁶⁰

No system can be made totally secure through technology. Typical security measures include user names and passwords, and user-specific menus to control access to certain functions (such as "view-only") and to limit the user's access to the information she actually needs.⁶¹ Audit trails may be used to trace the actions a user has performed on the system.⁶² Data encryption, digital signatures, and biometric identification can add additional levels of security.⁶³ In addition to technological safeguards, organizations generally have policies, training programs, and disciplinary procedures to assure in place that confidentiality is respected.⁶⁴

A major focus of such technical and procedural measures is to prevent breaches of confidentiality by authorized users.⁶⁵ "The potential for abuse of authorized internal access to information by persons within the system" is one of the greatest threats to medical information privacy.⁶⁶ However, because security measures are not

but the legal protections of information have not.

This section of this article is intended only to clarify the distinction between security issues and confidentiality or privacy issues, and to illustrate this distinction by highlighting some common security measures. A comprehensive discussion of system security is beyond the scope of this article. See PROTECTING PRIVACY, *supra* note 3, app. A at 89-99; NATIONAL RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE (1991); Stephen P. Heymann, *Legislating Computer Crime*, 34 HARV. J. ON LEGIS. 373 (1997).

59. See PROTECTING PRIVACY, *supra* note 3, app. A at 89-99.

60. See *id.*

61. See *id.* at 11.

62. See *id.*

63. See generally PROTECTING PRIVACY, *supra* note 3, app. A at 91-96.

64. See *id.* Unless security measures are accompanied by proper procedures and implementation, they cannot be effective. For example, Tom Rinfleisch, director of the Center for Advanced Medical Informatics at Stanford University, told NPR of places "where all doctors used the same log-in ID, and so it is not possible to ensure accountability for record use . . ." *Data Mining Regulations* (All Things Considered, National Public Radio broadcast, Aug. 26, 1997), available in WESTLAW, database ATCON, 1997 WL 12833303.

65. See PROTECTING PRIVACY, *supra* note 3, app. A at 90; see, e.g., *Arbster v. Unemployment Compensation Bd. of Review*, 690 A.2d 805, 810 (Pa. Commw. Ct. 1997) (affirming denial of unemployment compensation to a nurse who was discharged by her hospital-employer for violating the hospital's security policy by accessing confidential information from the hospital's computer about a family member undergoing treatment at the hospital).

66. PROTECTING PRIVACY, *supra* note 3, at 12.

foolproof, ethical and legal protections of medical information privacy are crucial.

V. ETHICAL PROTECTION OF THE RIGHT TO PRIVACY

Confidentiality of patient records is protected by the ethical obligations of health care providers. The concept of medical confidentiality may be as old as the practice of medicine.⁶⁷ The most widely known expression of a physician's obligation to maintain the confidentiality of patient information is the Hippocratic Oath.⁶⁸ The principle is echoed in modern codes of ethics as well. For example, the 1992 Code of Medical Ethics of the American Medical Association (AMA) details the obligations of physicians with regard to the confidentiality of patient information.⁶⁹

According to the AMA, information disclosed by a patient to a physician during the course of treatment should be accorded the greatest possible degree of confidentiality.⁷⁰ These principles hold physicians to a high standard of patient confidentiality; yet physi-

67. See Bernard Friedland, *Physician-Patient Confidentiality: Time to Re-Examine a Venerable Concept in Light of Contemporary Society and Advances in Medicine*, 15 J. LEGAL MED. 249, 256 (1994) (citing Kenneth McK. Norrie, *Medical Confidence: Conflicts of Duties*, 24 MED. SCI. & LAW 26 (1984)); see generally Robert M. Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 N.C. L. REV. 255, 267-71 (1984) (reviewing the development of codes of ethical principles in the medical profession).

68. See Friedland, *supra* note 67, at 256. The Hippocratic Oath is believed to date from around 400 B.C. See *id.* The Hippocratic Oath states: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about." *Id.* (citing LUDWIG EDELSTEIN, *THE HIPPOCRATIC OATH: TEXT, TRANSLATION AND INTERPRETATION* 3 (1943)). Various versions of the wording of this oath exist, based on different translations of the ancient Greek, but all contain the same essential element of confidentiality. See *id.* at 256 n.40 (citing Curley Bonds, *The Hippocratic Oath: A Basis for Modern Ethical Standards*, 264 JAMA 2311 (1990)).

69. See Donaldson & Lohr, *supra* note 45, at 148 (citing AMERICAN MEDICAL ASS'N, *PRINCIPLES OF MEDICAL ETHICS* § 5.05 (1992)).

70. See *id.* at 148. The AMA *Principles of Medical Ethics* provide in pertinent part:

The information disclosed to a physician during the course of the relationship between the physician and patient is confidential to the greatest possible degree The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law.

Id. (citing AMERICAN MEDICAL ASS'N, *PRINCIPLES OF MEDICAL ETHICS* § 5.05 (1992)).

cians are not the only type of provider of health care services today. Only about five percent of health care is now provided by physicians, compared to eighty-five percent earlier in this century.⁷¹ Fortunately, other health professional groups have also adopted formal codes or policies regarding the handling of medical records.⁷² For example, the American Nurses Association's code of ethics includes a requirement that nurses judiciously protect confidential information.⁷³ Psychologists and social workers also have codes of ethics which entail an obligation to respect the privacy of patients or clients.⁷⁴

Health care information is also often maintained by non-provider entities, such as insurance companies. These businesses are not bound by the same ethical standards as health care providers.⁷⁵ This is not to say that these entities are not trustworthy, but only that the traditional relationship of confidentiality that patients rely upon with health care providers is less certain with other business organizations.⁷⁶

Professional ethical codes do not impose legal obligations. As explained by the Missouri Supreme Court:

71. See UNIF. HEALTH-CARE INFORMATION ACT § 1-101 cmt., 9 pt. I U.L.A. 479, 481 (1988).

72. See UNIF. HEALTH-CARE INFORMATION ACT, prefatory note, 9 pt. I U.L.A. 475, 476 (1988). These include the American Hospital Association and the American Medical Record Association. See *id.*

73. See William H. Minor, *Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections*, 28 COLUM. J.L. & SOC. PROBS. 253, 279 n.139 (1995) (citing D. Kathy Milholland, *Privacy and Confidentiality of Patient Information*, J. NURSING ADMIN., Feb. 1994, at 19).

74. See Judith Larsen et al., *Medical Evidence in Cases of Intrauterine Drug and Alcohol Exposure*, 18 PEPP. L. REV. 279, 300 n.76 (1991) (citing American Psychological Ass'n, *Ethical Principles of Psychologists*, 36 AM. PSYCHOLOGIST 633, 635-36 (1981) ("Psychologists have a primary obligation to respect the confidentiality of information obtained from persons in the course of their work as psychologists."); CODE OF ETHICS OF THE NAT'L ASS'N OF SOCIAL WORKERS, § 1.07 ("Social workers should respect clients' right to privacy").

75. See Gostin et al., *supra* note 20, pt. 4, § VI.B. Most Americans have confidence that the health professionals they use are careful to keep medical information confidential. See Louis Harris & Assoc. Poll, Nov. 1993, available in WESTLAW, POLL database, File USHARRIS.93PRIV RC02D. Respondents were not asked about their confidence in insurance companies or other non-provider entities in the health care system. See *id.*

76. One insurance company representative stated that, overall, the insurance industry has a good track record in protecting information privacy. See, e.g., *Insurers Must Take Lead in Debate Over Privacy*, Nat'l Underwriter Life & Health—Fin. Servs. Edition, Oct. 27, 1997, at 68, available in WESTLAW, NATUNDLH database, 1997 WL 17014928.

While the ethical principles [of the Hippocratic Oath] may evidence public policy that courts may consider in framing the specific limits of the legal duty of confidentiality, this legal duty is to be distinguished from the ethical duty. The civil action for damages in tort is the sanction that puts teeth into the physician's duty of confidentiality.⁷⁷

Nevertheless, codes of professional ethics may be enforced through professional disciplinary procedures. Moreover, such ethical codes are important to the confidentiality of patient information, because many health care professionals may be more aware of the requirements imposed by their professional oaths than of the myriad of federal and state laws regarding confidentiality of medical information.⁷⁸

VI. FEDERAL LEGAL PROTECTIONS

A. *Constitutional Right to Privacy*

The United States Constitution does not expressly guarantee a right to privacy; however, the United States Supreme Court recognized a limited right to informational privacy in *Whalen v. Roe*.⁷⁹ This landmark case concerned disclosure of computerized individually-identifiable medical data.⁸⁰ In *Whalen*, the Court addressed the issue of whether the constitutional protections of privacy under the Fourteenth Amendment extend to the collection, storage and dissemination of medical information in government databases.⁸¹ A New York statute required physicians to disclose certain individually-identifiable data about prescriptions for drugs with a high potential for diversion into unlawful channels, and it provided for centralized computer storage of that information by the state

77. *Brandt v. Medical Defense Assocs.*, 856 S.W.2d 667, 671 (Mo. 1993).

78. *See generally* Gellman, *supra* note 61, at 280 (noting the conclusion of George J. Annas, associate professor of law and medicine at the Boston University Schools of Medicine and Public Health, that health professionals seldom know the privacy laws of their own states).

79. 429 U.S. 589 (1977).

80. *See id.* at 591.

81. *See id.* at 600-02.

health department.⁸² The Court recognized that although disclosure of medical information might adversely affect some patients, “disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice.”⁸³ The Court held that the potential effects of disclosure in this case, combined with the security measures taken with the data, were not sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment.⁸⁴ Nevertheless, the Court acknowledged “the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.”⁸⁵ Thus, *Whalen*, although recognizing the problem, has afforded little constitutional protection for the privacy of sensitive medical information.⁸⁶

The *Whalen* Court did not analyze the special problems created by the computerization of data⁸⁷ and took only a limited look at the level of security provided for the records.⁸⁸ The computer system and security measures at that time were relatively simple.⁸⁹ The power of database retrieval and analysis tools available in 1999 far exceed those that were available in the 1970s, and the type of security considered adequate in *Whalen* might no longer be considered to provide sufficient protection for medical data. Central storage, high-capacity portable magnetic media, database tools, and easy ac-

82. See *id.* at 592-93.

83. *Id.* at 602.

84. See *id.* at 603-04. The security measures included protecting the receiving room with a locked wire fence and alarm system, keeping the computer tapes in a locked cabinet, running the computer off-line so that it was not accessible from the outside, and limiting public disclosure of the information. See *id.* at 594.

85. *Id.* at 605.

86. See, e.g., *Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425 (1977). The Court in *Nixon*, only a few months after *Whalen*, also acknowledged a right to informational privacy, albeit a narrow one. See *id.* at 456. Former President Nixon challenged a statute requiring disclosure of presidential materials to government archivists for screening. See *id.* at 429-30. The court held that Nixon had a legitimate expectation of privacy in his *personal* communications. See *id.* at 457-58 n.19, 465. However, the Court balanced the limited intrusion of the screening against the president's status as a public figure and his lack of expectation of privacy in most of the materials, and upheld the statute requiring disclosure. See *id.* at 458-60, 465. Just as the Court in *Whalen* had emphasized the security measures taken by the health department, the *Nixon* Court emphasized “the unblemished record of the archivists for discretion.” *Id.* at 465.

87. See *Whalen*, 429 U.S. at 605-06.

88. See *id.* at 601-02.

89. See *id.* at 603-04; *supra* note 84.

cessibility of computerized information have increased the vulnerability of medical data to misappropriation and misuse.

A few years later, in *United States v. Westinghouse Electric*,⁹⁰ the Third Circuit Court of Appeals set forth factors to be used by a court in weighing an individual's privacy interest in personal medical information against the need for public agency access to the information.⁹¹ The *Westinghouse* court stated:

Thus, as in most other areas of the law, we must engage in the delicate task of weighing competing interests. The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.⁹²

This balancing has generally not favored the protection of individual informational privacy.⁹³

When medical information is maintained or disseminated

90. 638 F.2d 570 (3d Cir. 1980).

91. *See id.* at 578.

92. *Id.*

93. *Whalen* has generally been limited to its facts and has not been broadly applied to protect informational privacy. *See, e.g., Nixon*, 433 U.S. at 458-60 (acknowledging a legitimate expectation of privacy in personal communications, but holding that the public interest in disclosure outweighed that privacy interest); *Doe v. Southeastern Pa. Transp. Auth.*, 72 F.3d 1133, 1143 (3d Cir. 1995) (holding that the employer's need for access to employees' prescription drug records, for purposes of cost containment in a self-insured drug plan, outweighed the employees' interest in confidentiality); *Schachter v. Whalen*, 581 F.2d 35, 37 (2d Cir. 1978) (holding that a New York statute allowing medical records to be subpoenaed for investigations of licensed physicians did not infringe any constitutional rights to informational privacy since the information was crucial to implementation of a sound state policy). *But see, e.g., J.P. v. DeSanti*, 653 F.2d 1080, 1091 (6th Cir. 1981) (holding that the constitutional right of privacy does not extend so far as to require a balancing of government and private interests in every case). *See generally* Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 145-49 (1991) (comparing recent court decisions on informational privacy).

electronically, decisions about data privacy also involve striking another balance, "in this case between the individual's right to privacy against the cost of security, the inherent impediment security measures present to the ready accessibility of data, and the societal benefits of access to information."⁹⁴

In summary, the constitutional right to privacy does not provide reliable protection for medical data. *Whalen* has never been applied to provide protection to computerized health information. In addition, the constitutional right to privacy is limited to state action; therefore, unless the government is the collector or disseminator of the information, one must look elsewhere for protection of this information.

B. Federal Legislation

There is currently no comprehensive federal legislation that protects the right to privacy of individually-identifiable health care information. Legislation has been proposed in Congress, but as yet, none has been enacted.⁹⁵ There are, however, some federal statutes that do provide some protection for the privacy of medical information.

1. The Privacy Act of 1974

The federal Privacy Act of 1974 (Privacy Act)⁹⁶ was enacted to assure that the government will use fair information practices with regard to the collection, use and dissemination of individually-identifiable records.⁹⁷ One of Congress' main concerns was the in-

94. PROTECTING PRIVACY, *supra* note 3, at 6.

95. See *infra* Part IX.

96. Pub. L. No. 93-579, § 1, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (1994)). The Privacy Act was amended in 1988 by the Computer Matching and Privacy Protection Act of 1988, which regulates the "matching" of files by using an individual's personal identifier, such as a social security number. See Pub. L. No. 100-503, 102 Stat. 2507 (amending 5 U.S.C. § 552a(note)).

97. See U.S. DEP'T OF JUSTICE, FREEDOM OF INFORMATION ACT GUIDE & PRIVACY ACT OVERVIEW 323 (1992) [hereinafter FOIA GUIDE].

The enactment of legislation defining a "Code of Fair Information Practices" was recommended by the Department of Health, Education and Welfare in a 1973 report. See Lillian R. Bevier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protections*, 4 WM. & MARY BILL RTS. J. 455, 462-63 (1995) (citing generally REPORT OF THE SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, Pub. No. OS 73-94 (1973)). The principles proposed by this report were:

creasing use of computers and sophisticated information systems, and the potential abuse of such technology.⁹⁸

The Privacy Act prohibits disclosure by a government agency of "any record" contained in a "system of records" under the control of a government agency.⁹⁹ Agencies that collect data must notify the individual that data is being collected and the reason for its collection.¹⁰⁰ Individuals are permitted access to their data and have the right to correct errors.¹⁰¹ If an agency does not comply with the Privacy Act, civil remedies are available to the individual adversely affected.¹⁰² Criminal penalties are also available in the case of any agency employee who willfully discloses confidential information in contravention of the Privacy Act.¹⁰³

Nevertheless, in many circumstances, these records may be disclosed without the subject's consent.¹⁰⁴ The exceptions that al-

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to correct or amend a record of identifiable information about him.
4. There must be a way for an individual to prevent information about him obtained for collected for one purpose from being used or made available for other purposes without his consent.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability for their intended use and must take reasonable precautions to prevent the misuse of data.

REPORT OF THE SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, Pub. No. OS 73-94, at 41 (1973); *see also* Bevier, *supra*, at 463. The Privacy Act of 1974 incorporated the principles in its basic policy objectives. *See* 5 U.S.C. § 552 (a) (1994); FOIA GUIDE, *supra*, at 325; Bevier, *supra*, at 463.

98. *See* Thomas v. United States Dep't of Energy, 719 F.2d 342, 345 (10th Cir. 1983) (stating that the legislative history of the Privacy Act showed Congress was concerned with the increasing use of computers and the potential abuse of the technology); FOIA GUIDE, *supra* note 97, at 325. Congress was also concerned about illegal surveillance and investigations by federal agencies, such as those exposed as a result of Watergate. *See* FOIA GUIDE, *supra* note 97, at 325.

99. *See* 5 U.S.C. § 552a(b) (1994).

100. *See id.* § 552a(e)(3).

101. *See id.* § 552a(d).

102. *See id.* § 552a(g)(1).

103. *See id.* § 552a(i)(1) (providing that an employee or officer who willfully discloses confidential information to any person or agency not entitled to receive it shall be guilty of a misdemeanor and subject to a fine of up to \$5000).

104. *See id.* § 552a(b).

low disclosure nearly swallow the rule. For example, disclosures for “routine uses” do not require consent.¹⁰⁵ That is, no authorization by the subject is required for release of the information for uses compatible with the uses for which the data was collected.¹⁰⁶ Furthermore, the Privacy Act only applies to records held by a government agency.¹⁰⁷ No protection is provided for privately held information.¹⁰⁸ Hospitals operated by the federal government and private health care facilities or research institutions maintaining records under government contract are covered under the Privacy Act, but other health care institutions are not.¹⁰⁹

In addition, the Privacy Act may not cover treatment notes or other information not contained in a “system of records.”¹¹⁰ For example, in *Thomas v. United States Department of Energy*,¹¹¹ the Tenth Circuit held that a supervisor’s disclosure to co-employees that another employee had had a psychiatric evaluation was not violative of the Privacy Act, because that information was derived independently of the agency’s “system of records.”¹¹² It did not matter that identical information was also contained in the agency’s “system of records” or that the supervisor may have known that the information may have been in the agency’s “system of records.”¹¹³ The court reasoned that Congress’ concern was the misuse of computerized information.¹¹⁴ Therefore, medical notes, which are not commonly a part of the patient’s computer record, are not protected if they are not part of the medical records database.¹¹⁵ If they are made part of the database, they would be protected by the Privacy Act.

In summary, while the Privacy Act does provide protections for government-held computerized medical records, as with other privacy protections, it is limited in scope.

105. *Id.* § 552a(b)(3).

106. *See id.* § 552a(a)(7), (b).

107. *See id.* § 552a(a)(1), (f).

108. *See id.*

109. *See id.* § 552(f).

110. *See id.* § 552a(b) (providing conditions for disclosure of any record contained in a system of records). A “system of records” is a group of records from which information is retrieved by the name or social security number of an individual. *See id.* § 552a(a)(5).

111. 719 F.2d 342 (10th Cir. 1983).

112. *See id.* at 345-46.

113. *See id.*

114. *See id.* at 345.

115. *See* 5 U.S.C. § 552a(b) (1994).

2. Freedom of Information Act (FOIA)

Information that is required to be disclosed under the Freedom of Information Act (FOIA)¹¹⁶ is not otherwise protected by the Privacy Act.¹¹⁷ FOIA requires that information held by executive branch agencies be made available on request to the general public, subject to nine exemptions.¹¹⁸ These exemptions may allow a government agency to withhold personal medical information requested under FOIA. FOIA exemption six pertains to "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."¹¹⁹ This exemption will prevent disclosure of individually-identifiable medical information, unless there is a public interest which outweighs the privacy interest in nondisclosure.¹²⁰ The Supreme Court has construed this exemption broadly, allowing agencies to protect such information.¹²¹ However, the agency has the discretion, though not the duty, to withhold information that falls within one of the exemptions.¹²²

116. 5 U.S.C. § 552 (1994).

117. *See id.* § 552(b)(2).

118. *See id.* § 552(b). Exemption one pertains to national security matters. *See id.* § 552(b)(1). Exemption two covers internal personnel practices of an agency. *See id.* § 552(b)(2). Exemption three covers any information specifically exempted from FOIA under other statutes. *See id.* § 552(b)(3). Exemption four protects trade secrets, and commercial or financial information which is obtained from an individual and is privileged or confidential. *See id.* § 552(b)(4). Exemption five pertains to internal agency memoranda. *See id.* § 552(b)(5). Exemption six exempts from disclosure "personnel and medical files and similar files the disclosure of which would [be] a clearly unwarranted invasion of personal privacy." *Id.* § 552(b)(6). Exemption seven covers law enforcement records. *See id.* § 552(b)(7). Exemption eight pertains to agencies regulating financial institutions, such as the stock exchanges, and is intended to protect the security of financial institutions. *See id.* § 552(b)(8); FOIA GUIDE, *supra* note 97, at 219. Exemption nine concerns geological and geophysical data. *See* 5 U.S.C. § 552(b)(9).

119. *Id.* § 552(b)(6).

120. *See* FOIA GUIDE, *supra* note 97, at 134.

121. *See id.* at 133 (citing *Department of State v. Washington Post Co.*, 456 U.S. 595 (1982) (holding that in light of its legislative history Congress intended section 552(b)(6) to be interpreted broadly)); *see also* Gostin et al., *supra* note 20, pt. 7, § III.B.

122. *See* FOIA GUIDE, *supra* note 97, at 3 (citing *Chrysler Corp. v. Brown*, 441 U.S. 281, 293 (1979)).

3. Other Federal Legislation

Federal law also provides privacy protection for the records of patients in federally-assisted drug and alcohol treatment facilities.¹²³ Consent of the patient is required (with limited exceptions) before contents of the treatment records may be disclosed.¹²⁴ Privacy of research subjects is also protected by federal law. Human subject research conducted or supported by the federal government must comply with certain regulations, including making adequate provisions to protect the privacy of subjects and to maintain confidentiality of data.¹²⁵ A final illustration of targeted federal legislation is the Americans with Disabilities Act (ADA).¹²⁶ The ADA generally forbids employers from considering an employee's health status in making employment decisions.¹²⁷ All of these laws, however, apply in very limited circumstances.

In summary, the U.S. Constitution and federal legislation do not provide certain protection of privacy for health care information. The informational privacy rights recognized in *Whalen* have been narrowly applied, and at best, only apply to state action. The Privacy Act and FOIA provide good protection of information held by the government, but contain many gaps. Furthermore, no privacy protection is provided to health care information held by private entities. Other, very targeted, legislation may provide valuable protection of data in particular areas, but will leave other equally sensitive data with insufficient protection.

VII. STATE LEGAL PROTECTIONS

Health care has traditionally been considered a matter of state regulation.¹²⁸ The Tenth Amendment allows the states to regulate

123. See 42 U.S.C. § 290dd-2 (1994).

124. See *id.* § 290dd-2(b)(1).

125. See, e.g., 42 U.S.C. § 241(d) (1994) ("The Secretary may authorize persons engaged in biomedical, behavioral, clinical, or other research (including research on mental health . . .) to protect the privacy of individuals who are the subject of such research by withholding . . . identifying characteristics of such individuals."); 21 C.F.R. § 20.63(a) (1998) (requiring patient-identifying information in medical files of controlled-drug research subjects to be deleted before such files are made public).

126. 42 U.S.C. §§ 12101-12213 (1994).

127. See *id.*

128. See Françoise Gilbert, *Privacy of Medical Records? The Health Insurance Portability and Accountability Act of 1996 Creates a Framework for the Establishment of Security*

health care issues, including the protection of medical data privacy.¹²⁹ As a result, there is considerable variation from state to state in the privacy protection afforded to health care information.¹³⁰ The following sections first outline the types of protections available at the state level—from state constitutions, common law and legislation. There is then a brief discussion of the Uniform Health Care Information Act (UHCIA), which attempted to bring some uniformity to this area. Three states, California, Tennessee and Minnesota are then discussed in some detail, to provide an illustration of the continuing variation among states in protecting the confidentiality of health care data.

A. *Categories of State Privacy Protections*

1. *State Constitutional Protections*

More than a dozen states have adopted constitutional amendments designed to protect privacy interests.¹³¹ Nonetheless, constitutional privacy claims are uncertain under these provisions, because they primarily protect only against breaches of privacy by state action. Furthermore, individuals asserting a constitutional right of informational privacy are unlikely to obtain a remedy unless “the state fails to assert any significant interest or is particularly

Standards and the Protection of Individually Identifiable Health Information, 73 N.D. L. REV. 93, 93 (1997). Gilbert notes that:

In the past, most health care issues have been under the control of each of the fifty states. These matters were considered to be local in nature. The Tenth Amendment to the United States Constitution clearly grants each state the power to legislate health care issues, including the protection of medical records privacy.

Id.

129. See U.S. CONST. amend. X (“The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.”).

130. See generally TOMES, *supra* note 27 (providing survey of state medical privacy legislation); Gostin et al., *supra* note 20, pt. 1 (examining state and federal laws and noting the variability that exists between states).

131. See Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 498 (1995) (citing ROBERT E. SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 17-18 (1981)); see also Terri Finkfine, Note, *Let Technology Counteract Technology: Protecting the Medical Record in the Computer Age*, 15 HASTINGS COMM/ENT L.J. 455, 477-78 (1993) (citing to the constitutions of Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington).

careless in disclosing highly sensitive information."¹³²

2. State Common Law

States recognize a variety of common law claims related to breaches of confidentiality. Three major theories of recovery for wrongful disclosure of confidential information by a physician are: (1) the breach of a fiduciary duty of confidentiality; (2) the invasion of the right to privacy; and (3) the breach of an implied contract.¹³³

Under the first theory, a physician has a duty of confidentiality that arises out of the fiduciary relationship that exists between a treating physician and his or her patient.¹³⁴ In *Watts v. Cumberland County Hospital System, Inc.*,¹³⁵ the court stated that the health care provider (a marital and family therapist) had a duty to conform to certain standards of conduct set by his profession.¹³⁶ While the fiduciary duty of confidentiality is a legal claim recognized in some states, other states do not recognize it as a cause of action in the absence of statute, and there is no common law action for breach of duties inherent in the physician-patient relationship.¹³⁷

132. Gostin, *supra* note 131, at 498 n.211 (citing *Doe v. Borough of Barrington*, 729 F. Supp. 376 (D.N.J. 1990); *Woods v. White*, 689 F. Supp. 874 (W.D. Wis. 1988), *aff'd*, 899 F.2d 17 (7th Cir. 1990); *Carter v. Broadlawns Med. Ctr.*, 667 F. Supp. 1269 (S.D. Iowa 1987)).

133. See *Brandt v. Medical Defense Assocs.*, 856 S.W.2d 667, 670 (Mo. 1993) (describing the basis for a physician's duty of confidentiality, as found in other jurisdictions) (citing Lonette E. Lamb, Note, *To Tell or Not to Tell: Physician's Liability for Disclosure of Confidential Information About a Patient*, 13 CUMB. L. REV. 617 (1983)).

134. See, e.g., *Brandt*, 856 S.W.2d at 670 (holding that such a fiduciary duty exists, although in this case it was waived by the patient initiating malpractice litigation); *Horne v. Patton*, 287 So.2d 824, 827 (Ala. 1974) (recognizing physician has a qualified duty of confidentiality not to reveal confidences obtained through the physician-patient relationship). See generally *Hammonds v. Aetna Cas. & Sur. Co.*, 237 F. Supp. 96, 101-02 (N.D. Ohio 1965) (characterizing the physician-patient relationship as one of trust and confidence).

Although courts frequently cite the Hippocratic Oath and other codes of ethical behavior, only one state has classified breach of confidentiality as medical malpractice. See *Friedland, supra* note 67, at 254 (citing *Watts v. Cumberland County Hosp. Sys., Inc.*, 330 S.E.2d 242 (N.C. Ct. App. 1985)).

135. 330 S.E.2d 242 (N.C. Ct. App. 1985).

136. See *id.* at 250.

137. See, e.g., *Mikel v. Abrams*, 541 F. Supp 591, 598 (W.D. Mo. 1982) (holding that Missouri courts do not recognize a cause of action based solely on breach of a confidential doctor-patient relationship); *Stubbs v. North Mem'l Med. Ctr.*, 448 N.W.2d 78, 83 (Minn. Ct. App. 1990) (holding that tortious breach of a physician-patient relationship has never been expressly recognized as a cause of action in

Most states recognize a tort action for the invasion of privacy.¹³⁸ Invasion of privacy is the “unwarranted appropriation or exploitation of [an] individual’s personality, the publication of private concerns in which the public has no legitimate interest, or wrongful intrusion into his or her private activities.”¹³⁹ However, many courts have found that such a claim also requires wide public disclosure of the confidential information, which rarely occurs in medical records cases.¹⁴⁰

Claims basing civil liability on an implied contract between the physician and patient have been more successful. Under this theory, courts have held that there exists an implied contract between the physician and patient, wherein the physician promised not to reveal confidential information:¹⁴¹

Any time a doctor undertakes the treatment of a patient, and the consensual relationship of physician and patient is established, two jural obligations . . . are simultaneously assumed by the doctor. Doctor and patient en-

Minnesota).

138. See *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 234 (Minn. 1998) (recognizing that a vast majority of jurisdictions acknowledge some form of privacy right). Only North Dakota and Wyoming have not recognized a tort for the invasion of privacy. See *id.*; ROACH, *supra* note 40, at 205.

139. ROACH, *supra* note 40, at 205.

140. See, e.g., *Mikel*, 541 F. Supp. at 597. The *Mikel* court stated:

There must be evidence of publicity in the sense of a disclosure to the general public or likely to reach the general public, as opposed to ‘publication’ required in a defamation action, in order for plaintiff to make a submissible case of invasion of privacy by public disclosure of private facts.

Id. (quoting *Tureen v. Equifax*, 571 F.2d 411 (8th Cir. 1978)); see also *Clayman v. Bernstein*, 38 Pa. D. & C. 543, 546 (1940) (prohibiting a physician from using photographs of the patient’s facial development in connection with medical instruction). The *Clayman* court found that even taking the patient’s picture without her consent was an invasion of privacy. See *Clayman*, 38 Pa. D. & C. at 547. But see, e.g., *Humphers v. First Interstate Bank*, 696 P.2d 527, 533 (Or. 1985) (holding no invasion of privacy when physician revealed birth-mother’s identity to daughter).

141. See, e.g., *Hammonds v. Aetna Cas. & Sur. Co.*, 243 F. Supp. 793, 796-801 (N.D. Ohio 1965) (citing numerous examples of how public policy dictates that doctors obey their “implied promise of secrecy” to promote full disclosure by patients); *MacDonald v. Clinger*, 446 N.Y.S.2d 801, 802 (N.Y. App. Div. 1982) (“This physician-patient relationship is contractual in nature, whereby the physician, in agreeing to administer to the patient, impliedly covenants that the disclosures necessary to diagnosis and treatment of the patient’s mental or physical condition will be kept in confidence.”).

ter into a simple contract As an implied condition of that contract, . . . the doctor warrants that any confidential information gained through the relationship will not be released without the patient's permission.¹⁴²

Ethical standards of conduct which prohibit disclosure of confidential patient information have also been used as the basis for enforcing implied contracts between health care providers and patients.¹⁴³ Nevertheless, claims based on an implied contract between physician and patient may not be recognized in all states.¹⁴⁴

Another cause of action in tort, defamation, may be brought if medical data containing inaccurate information are disclosed to an unauthorized person, and the subject's reputation is adversely affected.¹⁴⁵ Yet the information contained in medical records is generally true, and truth is an absolute defense to defamation.¹⁴⁶

Under one or a combination of these tort causes of action, a patient may recover damages for the improper release of confidential medical information. However, as noted, these claims are often ineffective in medical records cases, and the causes of action are not recognized in all states. As a result, many states have passed legislation to address at least some of these confidentiality issues.

3. State Legislation

There is significant variation from state to state in the nature and quality of legislation regarding confidentiality of medical information. About twenty percent of the states have a comprehensive public data practices statute.¹⁴⁷ These comprehensive statutes are based on the federal Privacy Act and provide some assurance

142. *Hammonds*, 243 F. Supp. at 801.

143. *See id.* at 797 (holding that public policy demands that physicians maintain patient confidences, based in part, on the physicians' ethical codes "on which the public has a right to rely").

144. *See, e.g., Stubbs v. North Mem'l Med. Ctr.*, 448 N.W.2d 78, 82 (Minn. Ct. App. 1990) (holding that although "Minnesota has not expressly held that an implied contract can exist between a patient and their physician," such a contract might be found on the right facts).

145. *See* PROTECTING PRIVACY, *supra* note 3, at 15; *see also* ROACH, *supra* note 40, at 200-01; *Berry v. Moench*, 331 P.2d 814, 819 (Utah 1958) (questioning a physician's discretion in passing on derogatory information acquired in connection with patient treatment that may not have been true).

146. *See* ROACH, *supra* note 40, at 202.

147. *See* UNIF. HEALTH-CARE INFORMATION ACT, prefatory note, 9 pt. I U.L.A. 475, 475-76 (1988) (citing as examples data practices statutes from eight states).

that at least state-held medical data will not be disclosed to third parties without the patient's consent.¹⁴⁸

Two types of medical data privacy legislation are common to nearly every state. First, statutes in every state require some level of reporting of patient information to state public health or law enforcement agencies.¹⁴⁹ This type of state legislation governing public health data—the protections provided and disclosures permitted—are commonly found among statutes and regulations establishing the authority of public health agencies.¹⁵⁰ Second, virtually every state recognizes some type of provider-patient privilege.¹⁵¹ This is the patient's privilege to restrict his or her physician (or, in some states, other health care providers) from disclosing confidential medical information in judicial proceedings.¹⁵²

In addition, state acts regulating the practice of medicine by health care professionals, and the operation of hospitals and other health care institutions, frequently contain provisions limiting the unauthorized disclosure of confidential patient information.¹⁵³ These licensing or regulatory statutes also serve as a basis for imposing liability.¹⁵⁴ Other statutes may provide limited privacy protec-

148. *See id.*

149. *See id.* at 476. These statutes typically require reporting patient information relating to gunshot wounds or other violent injuries; contagious and infectious diseases; and occupational illness or injuries. *See id.*

150. *See* Gostin et al., *supra* note 20, pt. 4, § III.B. *See, e.g.*, CONN. GEN. STAT. ANN. § 19a-25 (West 1997).

151. *See* UNIF. HEALTH-CARE INFORMATION ACT, prefatory note, 9 pt. I U.L.A. 476 (1988). *See generally* TOMES, *supra* note 27 (providing survey of state medical privacy legislation).

152. *See* UNIF. HEALTH-CARE INFORMATION ACT, prefatory note, 9 pt. I U.L.A. 476 (1988). Because there was no physician-patient privilege at common law, this privilege exists only if there is a statute. *See id.*; *see, e.g.*, MICH. COMP. LAWS § 600.2157 (1986 & Supp. 1998) (“[A] person duly authorized to practice medicine or surgery shall not disclose any information that the person has acquired in attending a patient in a professional character, if the information was necessary to enable the person to [treat] the patient as a physician.”).

153. *See* Gostin, *supra* note 131, at 507.

154. *See, e.g.*, *Hammonds v. Aetna Cas. & Sur. Co.*, 243 F. Supp. 793, 797 (N.D. Ohio 1965) (citing “the State Medical Licensing Statute which seals the doctor's lips in private conversation.”); *Horne v. Patton*, 287 So.2d 824, 829 (Ala. 1973) (“When the wording of Alabama's state licensing statute is considered . . . public policy in Alabama requires that information obtained by a physician in the course of a doctor-patient relationship be maintained in confidence.”); *Simonson v. Swenson*, 177 N.W. 831, 832 (Neb. 1920) (sustaining a cause of action against a physician who betrayed the trust of a patient). *But cf.* *Moses v. McWilliams*, 549 A.2d 950, 956 (Pa. Super. Ct. 1988) (holding that Pennsylvania's medical licensing statute does not provide for an independent cause of action against the doctor for

tion in the areas of patient-provider privilege, or disease-specific statutes (for example, limiting disclosure of information related to HIV or mental illness).¹⁵⁵

State legislation usually focuses on the parties, and bases the confidentiality protections on who is holding the information, not what type of information is being held.¹⁵⁶ This focus has been considered necessary because of the impracticably broad scope of information privacy concerns.¹⁵⁷ Some confidentiality statutes impose a duty of confidentiality on non-provider parties holding the medical information. These statutes also focus on the identity of the party holding the information. For example, although most states do not regulate the informational practices of insurers,¹⁵⁸ "four states expressly require insurers to maintain the confidentiality of medical information that they receive."¹⁵⁹ New York is one of these exceptions; insurance companies receiving medical information for the purpose of making claims payments have a duty to ensure that this information is not disclosed to other parties.¹⁶⁰

4. *Exceptions to Confidentiality Regulation*

Despite common law and statutory protection for the confidentiality of medical records and other health care information, state laws also provide for a number of exceptions to these confidentiality rules. The most common exception is for medical diagnosis and treatment, and related administrative functions, such as billing and claims.¹⁶¹ Nearly all states also require reporting of sexually transmitted and other communicable diseases to public

money damages).

155. See Gostin, *supra* note 131, at 507-08; see generally, Gostin et al., *supra* note 20, pt. 5 (discussing the protection of HIV-related information). See, e.g., CONN. GEN. LAWS ANN. § 19a-584 (West 1997); IDAHO CODE § 39-610 (1998).

156. See UNIF. HEALTH-CARE INFORMATION ACT § 1-101 cmt., 9 pt. I U.L.A. 481 (1988). The Uniform Act also took this approach. See *id.*; see generally TOMES, *supra* note 27 (providing a guide to medical privacy legislation, almost all of which places the responsibility for privacy on individual health care providers).

157. See UNIF. HEALTH-CARE INFORMATION ACT § 1-101 cmt., 9 pt. I U.L.A. 481 (1988).

158. See Gostin, *supra* note 131, at 507 (citing G.B. TRUBOW, PRIVACY LAW AND PRACTICE § 801 (1987)); see also Burris, *supra* note 27, at 452 (recognizing that insurers are left largely unregulated even though technology available for databases is growing).

159. Gostin et al., *supra* note 20, pt. 4, § VII.

160. See *id.*

161. See TOMES, *supra* note 27, at 187-89.

health agencies.¹⁶² These exceptions are necessary for the public purposes of disease prevention and control.¹⁶³ All jurisdictions also make some exceptions to the confidentiality rules for the public purposes of medical research and education.¹⁶⁴ Such information may be limited to legitimate research or educational purposes, and researchers may be required to publish only non-individually-identifiable data.¹⁶⁵

Physicians and other health care providers may also have a duty to violate the confidentiality of medical records to protect third parties from danger.¹⁶⁶ For example, in *Tarasoff v. Regents of University of California*,¹⁶⁷ the court held that physicians have a legal duty to disclose significant risks posed by their patients to known third parties.¹⁶⁸ Finally, all jurisdictions require disclosure of confidential medical information under court order or subpoena.¹⁶⁹ The statutes may require special handling of these records to avoid improper disclosure.¹⁷⁰

B. *Uniform Health-Care Information Act*

Recognizing the lack of uniformity across states in the protection of the privacy of health care information, the National Conference of Commissioners on Uniform State Laws (NCCUSL) prepared the Uniform Health-Care Information Act (UHCIA) of 1985.¹⁷¹ Two states, Montana and Washington, have adopted this uniform act.¹⁷² NCCUSL found that:

[t]he movement of patients and their health-care infor-

162. *See id.* at 189-91

163. *See id.* at 189.

164. *See id.* at 194-95.

165. *See id.*

166. *See id.* at 191-93.

167. 551 P.2d 334 (Cal. 1976).

168. *See id.* at 351 (holding that a psychotherapist treating a mentally ill patient had a duty to warn the patient's former girlfriend that the patient had made threats against her).

169. *See* TOMES, *supra* note 27, at 196-97.

170. *See id.* at 196 (citing, as a common type of requirement, Mississippi law which requires subpoenaed hospital records to be enclosed in a sealed inner envelope identifying the case, then in an outer envelope; an affidavit from the custodian is also required, certifying the records).

171. UNIF. HEALTH-CARE INFORMATION ACT §§ 1-101 to 9-106, 9 pt. I U.L.A. 478 (1988).

172. *See* MONT. CODE ANN. § 50-16-502 to -553 (1996) (adopted in 1987); WASH. REV. CODE ANN. § 70.02.005 to .904 (West 1992) (adopted in 1991).

mation across state lines, access to and exchange of health-care information from automated databanks, and the emergence of multi-state health-care providers creates a compelling need for uniform law, rules, and procedures governing the use and disclosure of health-care information.¹⁷³

Under the UHCIA, public health information may be disclosed:

for statistical purposes; with written consent; to medical personnel as necessary to protect a patient's health or well-being; as provided in tuberculosis or STD laws; to other state or local health agencies for providing health services or promoting public health purposes; in child abuse proceedings; and where necessary to implement public health legislation or regulations.¹⁷⁴

In creating the UHCIA, the NCCUSL followed the lead of prior legislation and focused on the identity of the party holding the information, and it did not extend protections for health care information held by non-health care providers.¹⁷⁵

While truly uniform state laws would be a viable alternative to federal privacy legislation, the UHCIA has only been adopted in two states to date.¹⁷⁶ Furthermore, uniform acts are always subject to modification by state legislatures. Therefore, inconsistencies would be likely to remain, even if there were a wider adoption of the "uniform" act.

C. *State Privacy Laws: California, Tennessee and Minnesota*

The following three examples illustrate the range of approaches taken by the states to protect the confidentiality of medical information.

173. UNIF. HEALTH-CARE INFORMATION ACT § 1-101, 9 pt. I U.L.A. 479 (1988).

174. Gostin et al., *supra* note 20, pt. 4, § III.B (citing UHCIA).

175. *See* UNIF. HEALTH-CARE INFORMATION ACT § 1-101 cmt., 9 pt. I U.L.A. 480 (1988).

176. *See* MONT. CODE ANN. § 50-16-502 to -553 (1996); WASH. REV. CODE ANN. § 70.02.005 to .904 (West 1992).

1. *Privacy in California*

Common law causes of action for disclosure of medical information have been very limited in California. California has recognized a right of privacy that extends to medical information.¹⁷⁷ However, the courts require a disclosure of the information to the public in general or to a large number of persons.¹⁷⁸ The primary cause of the dearth of common law cases is probably the strong constitutional and statutory protections provided to informational privacy in California.

The California state constitution was amended in 1972 to provide an "inalienable right" to privacy.¹⁷⁹ The purpose of the amendment was to address increasing concerns about information being collected by government and business, especially the threat posed by the computerization of records.¹⁸⁰ This constitutional provision has been interpreted as extending to the protection of confidential medical information.¹⁸¹ Unlike most constitutional rights to privacy, the California Constitution extends this right to cover actions by private entities, not just governmental action.¹⁸²

The California court of appeal stated:

If the right of privacy is to exist as more than a memory or a dream, the power of both public and private institutions to collect and preserve data about individual citizens must be subject to constitutional control. Any expectations of

177. See *Schwartz v. Thiele*, 51 Cal. Rptr. 767, 770 (Cal. Dist. Ct. App. 1966) (holding, in an action by a woman against a physician who disclosed information about her mental health to a counselor, that California has recognized a justiciable right to privacy, i.e., "the right to be let alone").

178. See *id.* at 770-71 (holding that there was no invasion of privacy because there was no general "publication" of the information).

179. CAL. CONST., art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness and *privacy*.") (emphasis added). This 1972 amendment to the constitution was reworded in 1974. See *White v. Davis*, 533 P.2d 222, 233 n.9 (Cal. 1975).

180. See *White*, 533 P.2d at 233.

181. See *Division of Med. Quality v. Gherardini*, 156 Cal. Rptr. 55, 61 (Cal. Ct. App. 1979). The right to informational privacy is not absolute; however, it is a fundamental right, subject to strict scrutiny, and the government must show a compelling interest to invade that right. See *id.*

182. See *Hill v. National Collegiate Athletic Ass'n*, 865 P.2d 633, 644 (Cal. 1994); *Wilkinson v. Times Mirror Corp.*, 264 Cal. Rptr. 194, 202 (Cal. Ct. App. 1989).

privacy would indeed be illusory if only the government's collection and retention of data were restricted.¹⁸³

Thus, California provides strong constitutional protection to medical information, whether collected and maintained by the government or by private parties.

California is also one of the few states taking a comprehensive approach to legislation of the confidentiality of medical information.¹⁸⁴ First, the state enacted the Information Practices Act of 1977.¹⁸⁵ The legislature recognized a right to informational privacy, grounded in the state constitution.¹⁸⁶ The Information Practices Act limits the amount of personally-identifiable information that may be gathered by agencies of the state government,¹⁸⁷ and each agency is required to establish safeguards for the confidentiality of the data collected.¹⁸⁸ However, like the federal Privacy Act, the Information Practices Act protects the confidentiality of information only if held by the government.¹⁸⁹

California greatly expanded the explicit protections accorded to medical information with the Confidentiality of Medical Information Act (CMIA) in 1981.¹⁹⁰ The CMIA provides comprehensive guidelines regarding the disclosure of individually-identifiable

183. *Wilkinson*, 264 Cal. Rptr. at 200. Private conduct which impacts an individual's right to privacy need not be justified by a compelling interest (as with state action), but need only be reasonable, provided the privacy right is not "substantially burdened." *Id.* at 203.

184. *See Gostin, supra* note 131, at 506-07.

185. Act effective July 1, 1997, ch. 709, 1977 Cal. Stat. 2269 (codified as amended at CAL. CIV. CODE § 1798).

186. *See* CAL. CIV. CODE § 1798.1 (West 1982 & Supp. 1998). The legislature stated:

The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

Id.

187. *See id.* § 1798.14.

188. *See id.* § 1798.21.

189. *See id.* § 1798.3(b).

190. *See* 1981 Cal. Stat. ch. 782, § 1 (codified at CAL. CIV. CODE ch. 56 (West 1982 & Supp. 1998)). The California legislature recognized "that persons receiving health care services have a right to expect that the confidentiality of individual identifiable medical information derived by health service providers be reasonably preserved." *Id.*

medical information.¹⁹¹ The CMIA "is intended to protect the confidentiality of individually-identifiable medical information obtained from a patient by a health care provider, while at same time setting forth limited circumstances in which release of such information to specified entities or individuals is permissible."¹⁹²

The CMIA places a duty on physicians to maintain the confidentiality of patient records.¹⁹³ Records may not be released without the patient's prior written consent.¹⁹⁴ The CMIA sets forth the requirements of a valid authorization for the release of medical information by a provider of health care¹⁹⁵ or an employer.¹⁹⁶ Unauthorized release, which causes harm to the patient, is a misdemeanor.¹⁹⁷ Furthermore, the patient has a private cause of action against the violating party.¹⁹⁸

No protection of patient information from disclosure is absolute, and one of the virtues of the CMIA is that it makes the exceptions very clear. Providers *must* disclose medical information when compelled by a court order or administrative order of a state agency, or pursuant to a subpoena or search warrant.¹⁹⁹ Providers *may* disclose medical information to other health care providers for diagnosis or treatment.²⁰⁰ Permissive disclosure is also allowed to insurers, employers or health plans, to the extent necessary to pay claims;²⁰¹ to the provider's administrative service; peer review organizations; licensing or accrediting bodies; public agencies; bona

191. See CAL. CIV. CODE ch. 56.

192. *Loder v. City of Glendale*, 927 P.2d 1200, 1207 (Cal. 1997).

193. See CAL. CIV. CODE § 56.10 (West 1982 & Supp. 1998).

194. See *id.*

195. See *id.* § 56.11.

196. See *id.* § 56.21.

197. See *id.* § 56.36 (providing that "[a]ny violation of the provisions of this part which results in economic loss or personal injury to a patient is punishable as a misdemeanor"); CAL. CIV. CODE § 1798.57 (West 1998) (making it a misdemeanor to release medical information without the patient's consent, if the unauthorized release harms the patient).

198. See CAL. CIV. CODE § 56.35 (West 1982 & Supp. 1998) (providing that any patient whose medical information is used or disclosed in violation of the Confidentiality of Medical Information Act, and who suffers economic loss or personal injury as a result, may recover compensatory damages, punitive damages up to \$3000, costs, and attorney fees up to \$1000). See also *Pettus v. Cole*, 57 Cal. Rptr. 2d 46, 73-74 (Cal. Ct. App. 1996) (holding that the plaintiff's employer and two psychiatrists violated the CMIA by their disclosure and use of confidential medical information that resulted in the plaintiff's termination of employment).

199. See CAL. CIV. CODE § 56.10(b) (West 1982 & Supp. 1998).

200. See *id.* § 56.10(c)(1).

201. See *id.* § 56.10(c)(2).

fide researchers; and employers, if the treatment was at the request of and paid for by the employer.²⁰² Secondary disclosures of medical information are also limited; these authorized recipients of medical information may not further disclose it without a new authorization.²⁰³

Other regulations dictate the handling of medical information in specific facilities. Hospital and medical staff are required to establish a written policy on patient rights, including considerate and respectful care, full privacy concerning the medical care provided, and confidentiality of all medical records and other communications related to the patient's hospital stay.²⁰⁴ Patients in skilled nursing facilities have the right to confidential treatment of all financial and health records and must approve their release, except as otherwise authorized by law.²⁰⁵ Similar provisions also apply to acute psychiatric hospitals,²⁰⁶ intermediate care facilities,²⁰⁷ home health care agencies,²⁰⁸ primary care clinics,²⁰⁹ psychology clinics,²¹⁰ psychiatric health facilities,²¹¹ adult day health facilities,²¹² and chemical dependency recovery hospitals.²¹³

Other statutes provide additional protection for treatment involving certain conditions. Patient records related to treatment or rehabilitation for drug or alcohol abuse are given special protection.²¹⁴ The identity, diagnosis, prognosis and treatment of these patients are confidential and may only be disclosed under limited circumstances.²¹⁵ Special privacy protection rules also apply to psychiatric records.²¹⁶ Mandatory disclosure of psychiatric records oc-

202. *See id.* § 56.10(c)(3)-(8).

203. *See id.* § 56.13.

204. *See* CAL. CODE REGS. tit. 22, § 70707 (1998).

205. *See id.* § 72453(c).

206. *See id.* § 71551(a).

207. *See id.* § 73543(b).

208. *See id.* § 74731(b).

209. *See id.* § 75055(b).

210. *See id.* § 75343(b).

211. *See id.* § 77143(a).

212. *See id.* § 78433 (1997).

213. *See id.* § 79347(b).

214. *See* CAL. HEALTH & SAFETY CODE § 11977 (West 1991).

215. *See id.* For most medical treatment, such information is not considered confidential. In California, a provider may only disclose, without patient authorization, the patient's name, address, age, sex, general description of the reason for treatment, general nature of the injury, general condition of the patient, and any non-medical information. *See* CAL. CIV. CODE § 56.05(b) (West 1982 & Supp. 1998).

216. *See* CAL. WELF. & INST. CODE § 5328 (West 1998).

curs similarly to the disclosure of other medical records, e.g., to other providers, for claims payment purposes and research; however, each such disclosure must be documented in the patient's psychiatric record.²¹⁷ Similar provisions relate to the records of developmentally disabled patients.²¹⁸

In summary, common law claims related to medical privacy have been superseded by California's comprehensive constitutional and statutory protections for medical information. Furthermore, the focus of the legislation is still on the identity of the holder of the information.

2. *Privacy in Tennessee*

In stark contrast to California, Tennessee law provides little protection for the privacy of medical information. Although Tennessee does recognize a right of individual privacy under its state constitution,²¹⁹ this right is limited to state action, and furthermore, has not as yet been extended to encompass a right to informational privacy.

A review of Tennessee case law reveals no plaintiff prevailing in a common law action for invasion of privacy by public disclosure of private facts.²²⁰ Other common law causes of action are also lim-

217. See *id.* § 5328.6.

218. See *id.* §§ 4514, 4516.

219. See *Davis v. Davis*, 842 S.W.2d 588, 600 (Tenn. 1992). The *Davis* court recognized a constitutional right to procreational autonomy arising from the "right of individual privacy guaranteed under and protected by the liberty clauses of the Tennessee Declaration of Rights." See *id.* (referring to TENN. CONST. art. I, §§ 1-3, 7-8, 19, 27).

220. Only four Tennessee cases discussing claims for invasion of privacy by public disclosure of private facts were found. Search of WESTLAW, TN-CS database, for "invasion of privacy" and "public disclosure of private facts" (Jan. 10, 1999). See *Robinson v. Omer*, No. 01A01-9510-CV-00434, 1996 WL 274406, at *5 (Tenn. Ct. App. May 24, 1996) (finding for defendant due to lack of evidence that defendant gave plaintiff's name to anyone and because reporting illegal activity does not constitute "publicizing" private facts), *rev'd in part on other grounds*, 952 S.W.2d 423 (Tenn. 1997); *Major v. Charter Lakeside Hosp. Inc.*, No. 42, 1990 WL 125538, at *5 (Tenn. Ct. App. Aug. 31, 1990) (dismissing the claim for invasion of privacy because patient's name was only disclosed to one outside party); *Brooks v. Collinwood Church of God, C.A. No. 846*, 1989 WL 73232, at *3 (Tenn. Ct. App. July 6, 1989) (stating that Tennessee does not recognize a cause of action for public disclosure of private facts and that even if Tennessee recognized such a cause of action, the one-year statute of limitations applicable to actions for personal injuries had passed); *Gentry v. E.I. DuPont de Nemours & Co.*, C.A. No. 765, 1987 WL 15854, at *1 (Tenn. Ct. App. Aug. 18, 1987) (finding no invasion of privacy where private conversation between two parties which was inadvertently tape recorded

ited. Tennessee does not recognize a physician-patient privilege forbidding disclosure of confidential information to third parties.²²¹ The Tennessee Supreme Court, in *Quarles v. Sutherland*,²²² held that although physicians have an ethical duty to preserve patient confidentiality, this ethical requirement is not enforceable by law and cannot form the basis of a cause of action.²²³ The *Quarles* court suggested that a cause of action for improper disclosure by a physician of a patient's confidential information might be found under a theory of implied contract.²²⁴ This has not yet been tested in the Tennessee courts.

Statutory protection for health care information is also limited. Tennessee has a public records statute which classifies certain state-held records as confidential.²²⁵ Among the few categories of confidential information are the medical records of patients in state hospitals and medical facilities, and the medical records of persons receiving medical care at the expense of the state.²²⁶ But this statute does not apply to patients in private facilities where the state is not paying for the care.²²⁷

Tennessee does not have a general statute providing for the confidentiality of medical information. There are a few statutes related to confidentiality of medical records but, unlike the California statutes, they contain little information about the nature and scope of the protections given. For example, patients receiving care as an inpatient at a hospital or other licensed health care facility have the right to privacy in the care received, and release of identifying information will constitute an invasion of the patient's right to privacy.²²⁸ Exceptions apply to access by third-party payors for utilization review, case management, peer reviews and other administrative functions, and to access by other health care providers for diagnosis or treatment.²²⁹ A similarly worded provision, with

was heard by only a few company employees and then deleted, and the employees were instructed not to reveal the conversation to anyone).

221. See *Quarles v. Sutherland*, 389 S.W.2d 249, 251 (Tenn. 1965) (holding that there is neither a statutory nor common law physician-patient privilege).

222. 389 S.W.2d 249 (Tenn. 1965).

223. See *id.* at 251.

224. See *id.* at 252.

225. See TENN. CODE ANN. § 10-7-504 (1997 and Supp. 1998).

226. See *id.* § 10-7-504(a)(1).

227. See *id.*

228. See *id.* § 68-11-1503.

229. See *id.* § 68-11-1503; see also *id.* § 68-11-304 (stating that hospital records are not public records).

the same exceptions, can be found under the professional licensing statute; it applies to all medical records, and thus encompasses care provided in a clinic or doctor's office.²³⁰ The medical records of nursing home residents also must be kept confidential.²³¹ In addition, there is a provision in the Health Maintenance Organization Act that requires an HMO to maintain the confidentiality of patient/enrollee records.²³²

As in California, medical records related to certain specified conditions receive additional protection. Records related to sexually transmitted disease that are held by a public health department shall be "strictly confidential" and may be released only in limited circumstances, including subpoena, court order, and by authorization of the subject.²³³ Individually-identifiable medical records related to mental health patients are confidential and may be disclosed only under the limited circumstances specified in the statute.²³⁴ A physician performing an abortion must report it to the commissioner of health, but that record and report shall be confidential and not accessible to the public.²³⁵

In summary, the protections provided to medical information under Tennessee law are very limited under common law and statute. The few statutes that exist are less detailed than those of California, and they provide little guidance in determining the scope of protection accorded to medical information.

3. *Privacy in Minnesota*

Minnesota is mid-way between the approaches of California and Tennessee in terms of the privacy protections available for health care information. There is not a predominate comprehensive statute as in California; however, there are considerably more protections than in Tennessee.

The Minnesota Constitution does not explicitly provide a right to privacy. Nevertheless, in *State v. Gray*,²³⁶ the Minnesota Supreme Court noted that the Minnesota Bill of Rights recognizes a state constitutional right of privacy flowing from Article I of the Minne-

230. *See id.* § 63-2-101(b)(2).

231. *See id.* § 68-11-901(13), -910(3).

232. *See id.* § 56-32-225.

233. *See id.* § 68-10-113.

234. *See id.* § 33-3-104(10).

235. *See id.* § 39-15-203.

236. 413 N.W.2d 107, 111 (Minn. 1987).

sota Constitution.²³⁷ The court has yet to apply this constitutional right to protect individual privacy, and it is not clear whether such protections would extend to non-governmental action.

The common law has not provided clear privacy protection either. Until recently, Minnesota was one of only three remaining states which had never recognized the tort of invasion of privacy.²³⁸ In July 1998, in *Lake v. Wal-Mart Stores, Inc.*,²³⁹ the Minnesota Supreme Court reversed long-established precedent and recognized a cause of action for invasion of privacy.²⁴⁰ The court did not decide the case on its merits but remanded it to district court for reconsideration based on recognition of the cause of action.²⁴¹ It re-

237. See *id.* at 111-13; see generally, Michael K. Steenson, *Fundamental Rights in the "Gray" Area: The Right to Privacy Under the Minnesota Constitution*, 20 WM. MITCHELL L. REV. 383, 411 (1994) (concluding the privacy right in Minnesota has an uncertain future and it is unclear whether the court will decide to interpret the right of privacy under the Minnesota Constitution more broadly than the U.S. Constitution).

238. See *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 234 (Minn. 1998) (recognizing invasion of privacy as a cause of action). North Dakota and Wyoming are now the only states that have not recognized this tort. See *id.*

239. 582 N.W.2d 231 (Minn. 1998).

240. See *id.* at 236. There are four forms of the invasion of privacy tort—intrusion upon seclusion, appropriation of the name or likeness of another, publication of private facts, and false light publicity. See *id.* at 233 (citing the RESTATEMENT (SECOND) OF TORTS § 652E (1977)). The *Lake* court recognized a cause of action for the first three of these, but it declined to recognize a cause of action for false light publicity. See *id.* at 235. The court held that the tort of false light publicity was unnecessary due to its similarity to the recognized tort of defamation, and the court stated that risk of chilling free speech outweighed the limited additional protection that a tort of false light publicity would provide. See *id.* at 235-36.; see also Barbara E. Tretheway & Jeffrey J. Steinle, *Invasion of Privacy: Provider Liability for Disclosing Medical Records*, MINN. PHYSICIAN, Sept. 1998, at 18.

In 1975, the Minnesota Supreme Court had held that "Minnesota has never recognized, either by legislative or court action, a cause of action for invasion of privacy." *Hendry v. Conner*, 303 Minn. 317, 319, 226 N.W.2d 921, 923 (1975). This position was reiterated in 1996 in *Richie v. Paramount Pictures Corp.*, 544 N.W.2d 21, 28 (Minn. 1996). In *Lake*, the court characterized these prior statements denying recognition of an invasion of privacy tort as dicta. See *Lake*, 582 N.W.2d at 233 n.1. But it was dicta the Minnesota Court of Appeals consistently felt bound to follow. See *Lake v. Wal-Mart Stores, Inc.*, 566 N.W.2d 376, 378 (Minn. Ct. App. 1997) (noting that the plaintiffs had stated a "colorable claim" for invasion of privacy, but affirming dismissal of the claim because it felt bound by precedent to do so); see also *Stubbs v. North Mem'l Med. Ctr.*, 448 N.W.2d 78, 80-81 (Minn. Ct. App. 1989) (claiming it is not the courts' duty to establish new causes of action); *House v. Sports Films & Talents, Inc.*, 351 N.W.2d 684, 685 (Minn. Ct. App. 1984) (claiming that the court is bound by the state supreme court's observation that Minnesota has never recognized a cause of action for invasion of privacy).

241. See *Lake*, 582 N.W.2d at 236. *Lake* involved a nude vacation photograph

mains to be seen how Minnesota courts will judge the merits of invasion of privacy cases, in particular, claims involving medical records. The *Lake* ruling is a significant shift in Minnesota privacy law and will likely lead to more invasion of privacy claims. Until these claims have been heard by the Minnesota courts, the parameters of this new cause of action will remain unclear and the likelihood of plaintiff relief uncertain.

Minnesota has recognized the potential for another common law claim, based on an implied contract between a physician and patient.²⁴² The right facts have apparently never presented themselves though. No Minnesota appellate court has provided a remedy to a patient based on the physician's breach of an implied contract of confidentiality.²⁴³ Another possible common law claim, tortious breach of the fiduciary duty created by the physician-client relationship, has never been recognized as a cause of action in Minnesota.²⁴⁴

In summary, common law protections for medical data privacy in Minnesota have generally been ineffective. The apparent reluctance to apply common law protections to privacy may be explained in part by the existence of statutory alternatives.²⁴⁵ Minnesota law generally recognizes the importance of keeping medical information confidential.²⁴⁶ Although Minnesota has not taken a

of two women that Wal-Mart refused to develop. *See id.* at 233. Plaintiffs maintain that a Wal-Mart employee circulated the photograph in the community. *See id.*

242. *See Stubbs*, 448 N.W.2d at 82-83. In *Stubbs*, a patient brought action against a physician for unauthorized publication of "before" and "after" photographs of her cosmetic surgery. *See id.* at 79-80. The Minnesota Court of Appeals reversed the order for summary judgment on the patient's claim against the doctor for breach of an implied contract. *See id.* at 82-83. The court held that implied contracts are recognized in Minnesota. *See id.* at 82. Furthermore, although "Minnesota has not expressly held that an implied contract can exist between a patient and their physician . . . there appears to be no reason why such a contract could not be found on these facts." *Id.*

243. Search of WESTLAW, KEYCITE database, on *Stubbs v. North Mem'l Med. Ctr.*, 448 N.W.2d 78, 80-81 (Minn. Ct. App. 1989), headnote 9 (Jan 10, 1999).

244. *See id.* at 83; *see also Zagaros v. Erickson*, 558 N.W.2d 516, 524 (Minn. Ct. App. 1997) (noting that Minnesota has not yet recognized medical malpractice causes of action alleging tortious breach of fiduciary duty).

245. *See Marshall H. Tanick, New Developments in Privacy Law in Minnesota, in HOW TO ACCOMMODATE THE RIGHT TO PRIVACY, THE PUBLIC'S RIGHT TO KNOW AND THE GOVERNMENT'S NEED FOR INFORMATION* § III, at 4 (Minn. State Bar Ass'n CLE, Mar. 1998).

246. *See UHC Management Co. v. Fulk*, No. C8-95-39, 1995 WL 265052, at *2 (Minn. Ct. App. May 9, 1995).

California-style, comprehensive approach to privacy legislation, nevertheless, a number of state statutes codify privacy rights.

The Minnesota Government Data Practices Act (Data Practices Act)²⁴⁷ establishes comprehensive regulations governing state access to data and the protection of the privacy of data maintained by the state.²⁴⁸ Under the Data Practices Act, medical data is classified as private data.²⁴⁹ There are, however, numerous exceptions allowing dissemination of this medical information. For example, private data may be collected, used or disseminated for different reasons than the original reason for collection if approval is obtained²⁵⁰ (a potentially very broad exception). The name of the patient, admission date, general condition, and release date is generally public data.²⁵¹ Medical data may be disclosed pursuant to a court order²⁵² or to administer federal funds and programs.²⁵³

The Minnesota Health Data Institute (MHDI) is a public-private partnership created by the legislature to coordinate the collection and analysis of health care performance data.²⁵⁴ MHDI is required to develop "policies that reflect the importance of protecting the right of privacy of patients in their health care data"²⁵⁵ Individually-identifiable data collected by MHDI is classified as private data under the Data Practices Act, retains the private data classification, and cannot be disclosed.²⁵⁶

The Data Practices Act gives comprehensive guidance regarding the confidentiality of government-held data. However, like the federal Privacy Act, it can do nothing to protect the vast amounts of

247. MINN. STAT. ch. 13 (1996).

248. *See id.*; *see generally*, Donald A. Gemberling & Gary A. Weissman, *Data Privacy: Everything You Wanted to Know About the Minnesota Government Data Practices Act From "A" to "Z"*, 8 WM. MITCHELL L. REV. 573, 575 (1982).

249. *See* MINN. STAT. § 13.42, subd. 3 (1996). "Medical data" is data collected because an individual is a patient of a health care provider that is operated by the state (or state agency or political subdivision); data provided by a private health care facility; or data provided by or about the patient's relatives. *See id.* § 13.42, subd. 1(a).

250. *See id.* §§ 13.05, subd. 4(c), 13.42, subd. 3(a) (setting forth procedures).

251. *See id.* § 13.42, subd. 2.

252. *See id.* § 13.42, subd. 3(c).

253. *See id.* § 13.42, subd. 3(d).

254. *See id.* § 62J.451, subd. 1.

255. *Id.* § 62J.452, subd. 1.

256. *See id.* § 62J.452, subd. 2. MHDI is allowed to disclose individually-identifiable data to authorized research organizations, but only to the extent otherwise permitted by statute. *See* MINN. STAT. § 144.335, subd. 3a(a) (1996 & Supp. 1997).

medical data held by non-government entities. Furthermore, the legislature, "in balancing the public's right to know with the individual's right to privacy, has struck the balance in favor of the public."²⁵⁷

Minnesota legislation also protects privately-held medical information. The Patient's Bill of Rights provides that health care facilities must treat patients and residents with courtesy and respect, and must keep a patient's personal and medical records confidential, except when disclosure is required by third-party payor contracts, or in connection with department of health investigations, or as otherwise required by law.²⁵⁸ Although this provision conveys an intent to assure hospital and nursing home patients that their personal and medical records will be treated confidentially,²⁵⁹ little guidance is provided for the health care providers in implementing this provision. Moreover, only the records of persons receiving inpatient care are protected; the statute does not address confidentiality of records related to office visits or other outpatient care.²⁶⁰ Finally, the Patient's Bill of Rights statute does not create a private cause of action, but is enforceable only by action of the state department of health.²⁶¹

257. *Johnson v. Dirkswager*, 315 N.W.2d 215, 221 (Minn. 1982); see *Cowles Media Co. v. County of Itasca*, Nos. 31-CO-91-854, 31-CO-91-868, 1992 WL 430242, at *4 (Minn. Dist. Ct. July 16, 1992) (refusal to provide names and addresses upon request violated statute); see generally, Lauren Lonergan & Paul C. Thissen, *How to Handle Health and Medical Data*, in *THE RIGHT TO PRIVACY VS. THE PUBLIC'S RIGHT TO KNOW* (Minn. State Bar Ass'n CLE, Sept. 1995) (reviewing conflicts in the health care area).

258. See MINN. STAT. § 144.651, subd. 16 (1996).

259. See *id.* § 144.65, subd. 1. The legislative intent of the Patient's Bill of Rights is to "promote interests and well being of the patients and residents of health care facilities." *Id.*

260. See *id.* § 144.651, subd. 2 (defining "patient" as a person admitted to an acute care facility for at least 24 hours, and defining "resident" as a person admitted to a non-acute care facility). "Patients and residents shall be assured confidential treatment of their personal and medical records . . ." *Id.* § 144.651, subd. 16; see also *Stubbs v. North Mem'l Med. Ctr.*, 448 N.W.2d 78, 82 (Minn. Ct. App. 1989) (holding that the plaintiff's treatment at an outpatient surgery center fell outside the scope of section 144.651, both because the stay was for less than 24 hours and because the facility was not an inpatient facility). Any release of medical records outside the inpatient facility, under the Patient's Bill of Rights, must be in compliance with section 144.335 of the Minnesota Statutes. See MINN. STAT. § 144.657, subd. 16 (1996); *supra* text accompanying notes 262-67.

261. See *J.T.P. v. St. Paul Ramsey Med. Ctr.*, No. C8-96-1217, 1997 WL 65511, at *2 (Minn. Ct. App. Feb 17, 1997). "The statute does not indicate an intent to create a private remedy . . ." *Id.* at *3. The exclusive authority for enforcement of the Patient's Bill of Rights seems to be given to the state. See *id.* at *2; see also

The Access to Health Records provisions of section 144.335 of the Minnesota Statutes comprise the most comprehensive medical records privacy legislation in Minnesota.²⁶² Under this statute, the patient must consent to the release of medical records.²⁶³ Such consent is not required for the release of information to other providers for the treatment of the patient.²⁶⁴ Consent is normally valid for one year; but this limitation does not apply in the most common cases—i.e., release of patient records to consulting providers, or to an insurer or health plan for purposes of claims payment, fraud investigation, or quality of care review.²⁶⁵ Secondary release of medical information in individually-identifiable form without the patient's consent is prohibited, and recipients must establish adequate safeguards to protect the information from unauthorized disclosure.²⁶⁶ Violations of these confidentiality and consent provisions "may be grounds for disciplinary action against a provider by the appropriate licensing board or agency."²⁶⁷ However, this does not provide the patient whose records are inappropriately released with any private cause of action.

Section 144.053 of the Minnesota Statutes protects research data.²⁶⁸ Research data held by or in conjunction with the Minnesota Department of Health for the purpose of reducing morbidity or mortality is confidential and shall be used only for the purposes of scientific or medical research.²⁶⁹ Any person participating in the research who discloses the information other than in strict conformity with the research project shall be guilty of a misdemeanor.²⁷⁰ Additional privacy protection is accorded subjects of alcohol or drug abuse research by the state.²⁷¹

Other statutes and rules control other aspects of data privacy, such as: disclosure to the Commissioner of Health of medical data

MINN. STAT. § 144.652(2) (1996) (providing authority to issue correction orders for substantial violations); *Stubbs*, 448 N.W.2d at 83 (concurring that section 144.651 does not provide a private cause of action).

262. See MINN. STAT. § 144.335 (1996 & Supp. 1997).

263. See *id.* § 144.335, subd. 3a.

264. See *id.* § 144.335, subd. 3a(b)(2).

265. See *id.* § 144.335, subd. 3a(c).

266. See *id.* § 144.335, subd. 3a(c).

267. *Id.* § 144.335, subd. 6.

268. See *id.* § 144.053.

269. See *id.* § 144.053, subd. 1.

270. See *id.* § 144.053, subd. 4.

271. See *id.* § 254A.09.

on individuals who are believed to pose a health threat;²⁷² data collected by health maintenance organizations;²⁷³ and confidentiality of patient records in nursing homes.²⁷⁴ Finally, Minnesota has a statutory physician-patient privilege.²⁷⁵

Finally, as in other state and federal statutes, Minnesota provides specific protections based on the patient's condition. Sexually transmitted disease information must be kept confidential.²⁷⁶ Records of treatment for alcohol and drug abuse, and records of employee drug and alcohol testing are confidential.²⁷⁷ Revealing a communication from or relating to a mental health patient is prohibited conduct for mental health practitioners.²⁷⁸

While Minnesota provides certain statutory protections for the confidentiality of medical records, it is a patchwork of provisions, making assessment of the rights and responsibilities of the parties difficult to determine. In addition, the private causes of action for violation of these statutes are limited.

In summary, as illustrated in this three-state example, there is considerable variation in the protections available for information privacy from state to state. This fact, combined with the increased frequency of interstate transfers of medical information, suggest the best approach is comprehensive privacy legislation at the federal level.

VIII. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted August 21, 1996.²⁷⁹ Among the main purposes of the Act were "to improve portability and continuity of health insurance coverage . . . to combat waste, fraud and abuse . . .

272. See *id.* §§ 144.4175, .4184, .4186; MINN. R. 4605.7000 to .7300 (1997).

273. See MINN. STAT. § 62D.14, subd. 4 (1996).

274. See MINN. R. 4655.3500 (1997).

275. See MINN. STAT. § 595.02, subd. 1(d), (g) (1996).

276. See MINN. R. 4605.7702 (1997).

277. See MINN. STAT. §§ 254A.09, 181.954 (1996).

278. See *id.* § 148B.68(k).

279. Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, and 42 U.S.C.). For an excellent analysis of key features of HIPAA, see Jack A. Rovner, *Analysis of the Provisions of the Health Insurance Portability and Accountability Act of 1996*, 9:3 HEALTH LAW. 1 (1996). See generally Gilbert, *supra* note 128 (reviewing the privacy implications of HIPAA).

and to simplify the administration of health insurance”²⁸⁰ Title II of the Act focuses on preventing fraud and abuse, and on administrative simplification.²⁸¹ The purpose of “administrative simplification” is to improve the Medicare and Medicaid programs, as well as the efficiency and effectiveness of the health care system.²⁸² Section 262 requires that the Department of Health and Human Services develop and implement standards for the electronic transmission of certain health information; section 264 further requires federal legislation or regulations to protect the confidentiality of individually-identifiable health information.²⁸³

HIPAA required the Secretary of Health & Human Services to study the privacy issues related to individually-identifiable health information and make detailed recommendations to Congress.²⁸⁴ These recommendations were made in September 1997.²⁸⁵ Congress is directed by HIPAA to enact legislation adopting standards with respect to the privacy of individually-identifiable health information which is to be transmitted electronically pursuant to section 262.²⁸⁶ If such legislation is not adopted by August 21, 1999, the Secretary of Health and Human Services will have an additional six months to promulgate final regulations containing such standards.²⁸⁷ So, one way or the other, standards for privacy of individually-identifiable medical information are to be adopted by February 21, 2000. Furthermore, the violation of those standards will carry significant penalties. Wrongful disclosure of individually-identifiable health information will result in a fine of up to \$50,000,

280. Pub. L. No. 104-191, preface, 110 Stat. at 1936.

281. *See id.* §§ 200–271 (Title II). Title I amends the Employee Retirement Income Security Act of 1974 (ERISA), adding provisions regarding health plan portability, availability and renewability. *See id.* §§ 101–195. Title III amends the Internal Revenue Code, creating Medical Savings Accounts, and providing deductions for health insurance costs and new provisions related to long-term care. *See id.* §§ 300–371. Title IV provides for application and enforcement of the group health plan requirements. *See id.* §§ 401–421. Title V focuses on revenue offsets. *See id.* §§ 500–521.

282. *See id.* § 261.

283. *Id.* §§ 262, 264 (codified at 42 U.S.C. §§ 1320d-2 to 1320d-8).

284. *See id.* § 264.

285. *See infra* Part IX for a discussion of these recommendations.

286. *See* Pub. L. No. 104-191, § 264(c), 110 Stat. at 2033 (codified at 42 U.S.C. § 1320d-2).

287. *See id.*; *see also* *Milestones in Health Information Standards* (last updated Aug. 14, 1998) <<http://aspe.os.dhhs.gov/admnsimp/asmiles.htm>>; *Milestones in Health Information Privacy* (last updated Dec. 1, 1998) <<http://aspe.os.dhhs.gov/admnsimp/pvcmls.htm>> (tracking the DHHS milestones for setting standards for electronic data and for privacy protections).

imprisonment for one year, or both.²⁸⁸ If the disclosure is malicious or for pecuniary gain, the penalties will be significantly higher (fine up to \$100,000; five years imprisonment).²⁸⁹

HIPAA has raised new privacy concerns through its mandate of the use of electronic data formats, because the implementation of data standards may make unauthorized access easier.²⁹⁰ Certainly, continuing advances in technology and increasing use of electronic data will fuel the privacy debate. At the same time, HIPAA will also provide the impetus to achieve a sorely needed federal standard for privacy of medical information.

IX. PROPOSED FEDERAL PRIVACY LEGISLATION

Health care regulation has traditionally been left to the states.²⁹¹ With modern computer technology and telecommunications, and the increasing frequency of exchange of medical information across state borders, the protection of health care information arguably becomes an interstate commerce issue.²⁹² Thus, it becomes a matter to be addressed at the federal level.

In the 1970s, Congress addressed some privacy concerns by enacting the Privacy Act of 1974.²⁹³ Congressional attention to privacy issues "virtually disappeared in the 1980s."²⁹⁴ The interest in privacy issues resurfaced in the 1990s, with President Clinton's

288. See Pub. L. No. 104-191, § 262(a), 110 Stat. at 2029 (codified at 42 U.S.C. § 1320d-6).

289. See *id.*

290. See, e.g., Rovner, *supra* note 279, at 7; John Schwartz, *Health Insurance Reform Bill May Undermine Privacy of Patients' Records*, WASH. POST, Aug. 4, 1996, at A23.

291. See *supra* notes 128-29 and accompanying text.

292. See Gilbert, *supra* note 128, at 94.

293. See *supra* Part VI.B.1. As part of the Privacy Act of 1974, Congress established the Privacy Protection Study Commission, which issued its report in 1977. See FOIA GUIDE, *supra* note 97, at 323. Although this was still the early days of the computerization of records, the Commission found that providers already had diminished control over medical records, that complete restoration of control was not possible, and that "voluntary patient consent to disclosure is generally illusory." George J. Annas, *Privacy Rules for DNA Databanks: Protecting Coded Future Diaries*, 270 JAMA 2346, 2348 (1993) (citing PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) [hereinafter PERSONAL PRIVACY]). The Commission's report made recommendations regarding the disclosure of medical data and the authorizations that should be required, but these recommendations were never generally adopted. See *id.* at 2349 (citing PERSONAL PRIVACY).

294. Annas, *supra* note 293, at 2349.

health care reform initiatives. Clinton's Health Security Act did not include comprehensive federal privacy protections; however, it would have required the National Health Board to propose such legislation within three years.²⁹⁵ During this period, there were a number of other health care privacy protection bills proposed, but none of these measures were passed.²⁹⁶ Attention has once again

295. See Minor, *supra* note 73, at 289-90.

296. See *id.* These bills included:

The Fair Health Information Practices Act of 1994, sponsored by Representative Gary Condit (D-Cal.). See *id.* at 290-91. This bill proposed a uniform federal code of fair information practices that would apply to individually-identifiable health data. See *id.* It would have created categories of "protected health information" and "health information trustees" to balance the public need for disclosure against the individual's right to privacy. *Id.*

The Health Care Privacy Protection Act of 1994, sponsored by Senator Patrick Leahy (D-Vt.). See *id.* at 291. This Senate bill was modeled after Condit's House bill, but with stricter provisions on researcher access, and more lenient provisions for law enforcement and government access, and stricter civil and criminal penalties. See *id.* at 291, 291 n.214.

The Health Care Information Modernization and Security Act of 1993, sponsored by Senators Christopher Bond (R-Mont.) and Donald Riegle (D-Md.) and Representatives Thomas Sawyer (D-Ohio) and David Hobson (R-Ohio). See *id.* This bill originated with the industry-based Working Group for Electronic Data Interchange (WEDI) and focused on setting standards for transmitting health care data among systems. See *id.*

In 1995, Senator Bennett introduced a widely discussed privacy bill—Senate Bill 1360, The Medical Records Confidentiality Act of 1995. S. 1360, 104th Cong. (1995). The bill required that protected health information not be disclosed or used except for the purposes for which it was collected, or related purposes. See S. 1360, 104th Cong. § 201(b)(1). Authorization of the patient was required for disclosure; however, exceptions were made for disclosure of non-individually-identifiable data, disclosures to next of kin, emergency treatment, disclosures to a health oversight agency and public health agencies, health research, and disclosures under subpoena or warrant. See *id.* §§ 202–212. As a result of all these exceptions, the Bennett bill was regarded by privacy advocates as providing too little protection. See Marguerite B. Griffith, *Senate Attempts to Regulate the Confidentiality of Medical Records*, 43 Hous. Law., Sept./Oct. 1996, at 10-11. Of particular concern were the provisions allowing broad disclosure, without authorization, to researchers, public health agencies, and law enforcement agencies. See *id.*; see also Charles Marwick, *Increasing Use of Computerized Recordkeeping Leads to Legislative Proposals for Medical Privacy*, 276 JAMA 270, 270-72 (1996) (quoting Lawrence Gostin).

Health law expert George Annas also criticized the Bennett bill as focusing on facilitating establishment of large medical databanks. See Phillip McAfee, *Medical Records Bill Would Create National Standards for Access, Privacy*, West's Legal News, Health Law Medical Records, Dec. 4, 1995, available in WESTLAW, WLN 4127, at 1995 WL 907249 (quoting Annas). One of the goals of the Bennett bill was to "promote the efficiency and security of the health information infrastructure [to] more effectively exchange and transfer health information" in a manner that will assure confidentiality. S. 1360, 104th Cong. § 2.

Senate Bill 1360 would have pre-empted state privacy laws, with excep-

focused on the need for federal privacy protections for health information. Congress, in enacting HIPAA, recognized that it needs to take action in this area.

This section will review the recommendations made by Donna Shalala, the Secretary of the U.S. Department of Health & Human Services (the "Secretary"), pursuant to HIPAA. Then it will analyze some of the key issues, as addressed by the Secretary and by health information privacy bills introduced in the 105th Congress, sponsored by Senator Leahy, Representative Condit, Representative McDermott, and Senator Bennett.²⁹⁷ The discussion of these current proposals is for the purpose of highlighting certain key issues and is not intended to be comprehensive. The bills now before Congress will continue to be debated and modified as the hearings continue on this complex issue.

tions made for certain state statutes, such as those protecting mental health records or provider-patient privileges. *See id.* § 401. Some commentators criticized this provision, arguing that state laws should not be pre-empted if they provided greater protection than the federal law. *See Griffith, supra*, at 10. Finally, the Act would have been enforced by the Department of Health and Human Services; the ACLU contended that this created a conflict of interest, because the department, as an administrator of health services (Medicare and Medicaid), would also have been subject to the Act. *See id.*

297. *See* Medical Information Privacy and Security Act, S. 1368, 105th Cong. (1997) (sponsored by Sen. Patrick Leahy (D-Vt.)); Fair Health Information Practices Act of 1997, H.R. 52, 105th Cong. (1997) (sponsored by Rep. Gary Condit (D-Cal.)); Medical Privacy in the Age of New Technologies Act, H.R. 1815, 105th Cong. (1997) (sponsored by Rep. Jim McDermott (D-Wash.)).

Senator Robert Bennett (R-Utah) introduced a long-awaited revised medical privacy bill on October 9, 1998. *See* 144 Cong. Rec. S12164 (daily ed. Oct. 9, 1998) (statement of Sen. Robert Bennett). Senator Bennett's bill was introduced as legislation to ensure confidentiality of medical records and healthcare-related information. *See id.*; *see also* S. 2609, 105th Cong. (1998). This bill was to have been released February 25, 1998, "but its introduction was delayed because critics said it contained loopholes that would allow marketers to make use of medical and prescription information." *See* Robert O'Harrow, Jr., *Panel to Start Hearings on Medical Data; Bill Would Streamline Privacy Protections*, WASH. POST, Feb. 26, 1998, at E4; *see also* *Medical Records Measure Delayed*, CONGRESS DAILY AM, Feb. 25, 1998, available in WESTLAW, CONGDAM, 1998 WL 9511973 (recognizing delay in introduction of bill so sponsors could revisit various provisions).

Other proposed bills target more specific areas of confidentiality. *See, e.g.*, Genetic Information Disclosure Restriction, H.R. 2215, 105th Cong. (1997) (restricting employers in obtaining, disclosing, and using genetic information); Data Privacy Act, H.R. 2368, 105th Cong. (1997) (promoting privacy of interactive computer services). Discussion of these bills is beyond the scope of this article.

A. *Recommendations of the Secretary of Health & Human Services*

As required under HIPAA, Secretary Shalala, presented recommendations to Congress concerning the confidentiality of individually-identifiable health information in September 1997.²⁹⁸ The secretary's recommendations will be used herein as a framework for discussion of key issues and current legislative proposals concerning federal protections for health information privacy.

The Secretary's recommendations are based on five key principles:

Boundaries. An individual's health care information should be used for health purposes and only those purposes, subject to a few carefully defined exceptions. . . . [Federal law] should impose a legal duty of confidentiality on [entities that receive health information].

Security. Organizations to which we entrust health information ought to protect it against deliberate or inadvertent misuse or disclosure. . . .

Consumer Control. Patients should be able to see what is in their records, get a copy, correct errors, and find out who else has seen them. . . .

Accountability. Those who misuse personal health information should be punished, and those who are harmed by its misuse should have legal recourse. . . .

Public Responsibility. Individuals' claims to privacy must be balanced by their public responsibility to contribute to the common good, through use of their information for important, socially useful purposes, with the understanding that their information will be used with respect and care and will be legally protected. Federal law should identify those limited arenas in which our public responsibilities warrant authorization of access to our medical information, and should sharply limit the uses and disclosure of information in those contexts.²⁹⁹

The detailed recommendations developed by the Secretary

298. See *Medical Records Privacy: Hearings Before Senate Comm. on Labor & Human Resources*, 105th Cong. (Sept. 11, 1997) (testimony by Donna E. Shalala, Secretary, U.S. Dep't of Health & Human Servs.), available in WESTLAW, CONGTMY, 1997 WL 14150648; SHALALA REPORT, *supra* note 1.

299. SHALALA REPORT, *supra* note 1, § I(D).

based on these principles will be divided for discussion into seven issues: Balancing Private Rights and Public Purposes, Scope of Action, Patient Access to Records, Informed Consent, Disclosures for Public Purposes, Penalties/Sanctions, and Federal Pre-emption.

B. Current Issues in Legislating Health Information Privacy

1. Balancing Private Rights and Public Purposes

Secretary Shalala's recommendations attempt to "steer a course between two extreme convictions."³⁰⁰ While protecting the privacy of people seeking health care, legislation must also permit socially important uses for health care information for the benefit of all society.³⁰¹ Finding the right balance is difficult and complex. The bills currently before Congress all seek to find this balance,³⁰² though the fulcrum will be positioned differently for each one. Representative Condit, introducing his privacy bill in Congress, characterized as a luxury the elevation of privacy rights above all societal interests.³⁰³ Such an imbalance, according to Condit, would be "impractical, unrealistic, and expensive."³⁰⁴ At the same time, the first section of Condit's bill states unequivocally that the "right to privacy is a personal and fundamental right"³⁰⁵ This need to balance the privacy needs of the individual, the public's need for disclosure, and the in the interests of many different stakeholders will make the task of enacting medical privacy legislation a great challenge.

2. Scope of Action

The scope of the Secretary's recommendations is limited to regulating information held by health care providers and payors,³⁰⁶ and those receiving information from them.³⁰⁷ This includes "serv-

300. *Id.*

301. *See id.*

302. *See, e.g.*, 143 CONG. REC. E30-02 (Jan. 7, 1997) (statement of Rep. Gary A. Condit).

303. *See id.* at E31.

304. *Id.*

305. H.R. 52, 105th Cong. § 2 (a) (1) (1997).

306. Health care payors include insurance companies, Blue Cross/Blue Shield plans, managed care companies, government plans (e.g., Medicare, Medicaid), and employer-sponsored plans. *See* SHALALA REPORT, *supra* note 1, § II(A)(1).

307. *See* SHALALA REPORT, *supra* note 1, § I(E).

ices organizations," such as claims processors, billing services, and similar organizations that have contractual relationships with providers or payors.³⁰⁸ These parties (sometimes referred to as "health information trustees") would not need to obtain patient authorization to collect patient data.³⁰⁹

The position of the AMA is that the medical record is the property of the provider and maintained for the primary purpose of providing a reliable tool for medical care and treatment; therefore, the health care provider should be the only "trustee" of the medical record.³¹⁰ The views of the AMA are highlighted throughout the following discussion because the physician, in particular, is often the person who creates the medical record, and in whom the patient places his or her trust that such information will be kept confidential.³¹¹

The congressional proposals from Condit and McDermott apply broader definitions of "health information trustees," controlling disclosure by health care providers, health oversight agencies, health benefit plan sponsors, public health authorities and health researchers, and others, not just providers and payors.³¹² In fact,

308. See *id.*

309. See *id.* § II(A)(1).

310. See *Medical Records Privacy: Hearings Before Senate Comm. on Labor & Human Resources*, 105th Cong. (Sept. 11, 1997) (statement by Donald J. Palmisano, member of the Board of Trustees of the American Medical Association), available in WESTLAW, CONGTM, 1997 WL 14152616 [hereinafter AMA Statement]; Massachusetts Medical Society, *Massachusetts Medical Society Policy: Patient Privacy and Confidentiality: Position of the American Medical Association* (visited Jan. 18, 1999) <<http://www.massmed.org/physicians/pubs/privacy/priv11.html>> [hereinafter MMS Policy]; *AMA-News Editorial, Preserve and Protect Patient Privacy*, AM. MED. NEWS, Dec. 8, 1997 (visited Jan. 18, 1999) <http://www.ama-assn.org/sci-pubs/amnews/amn_97/edit1208.htm> [hereinafter AMA Editorial].

311. See AMA Statement, *supra* note 310; AMA Editorial, *supra* note 310. In the view of the AMA, "[t]he rapid advances in electronic technology to collect, sort and analyze patient data place new stresses on patient privacy, but the changes do not diminish physicians' ethical obligation." AMA Editorial, *supra* note 310. Neither "efficiency" nor "technological potential" justify retreat from the rigorous standard of confidentiality required by the medical profession's ethical code. *Id.*

The AMA approach to federal legislation on medical data privacy is based on three principles: (1) patients have a basic right to privacy of their medical information; (2) patient privacy should be honored unless waived by non-coercive informed consent, or required by a very strong public interest; and (3) medical information, when disclosed, should be limited to only that information necessary to meet the specific and immediate purpose. See *id.*; AMA Statement, *supra* note 310; MMS Policy, *supra* note 310.

312. See H.R. 52, 105th Cong. §3(b)(5) (1997); H.R. 1815, 105th Cong. § 3(7) (1997).

Condit cited as perhaps the most important feature of his bill, that as the data moves throughout the health care system (and beyond), it would remain subject to this Act, regardless of who is holding the information.³¹³ This approach corrects one of the shortcomings of previous legislation, which controlled disclosure narrowly based on who was holding the information.

Lawrence Gostin and other commentators have suggested that because location means little in the world of electronic records and communications, the focus of privacy protection needs to shift from the institution creating the health records to the record itself.³¹⁴ Rather than establishing a single rule regarding disclosure or privacy, based on who created the record, the law must now develop more complex standards. Congress must create regulations that can respond to the different contexts in which medical data are used.

3. *Patient Access to Records*

The intent of the Secretary's recommendations is "to incorporate basic fair information practices into the health care setting."³¹⁵

313. See 143 CONG. REC. E30-02, E31 (1997).

314. See Gostin et al., *supra* note 31, at 8.

315. SHALALA REPORT, *supra* note 1, § I(G). The merits of these Fair Information Practices principles are well-accepted, at least in the abstract. Lawrence Gostin has identified certain practices following from these principles which should be a part of any federal privacy initiative:

- (i) information should be collected only to the extent necessary to carry out the purpose for which the information is collected;
- (ii) information collected for one purpose should not be used for another purpose without the individual's informed consent;
- (iii) information should be disposed of when no longer necessary to carry out the purpose for which it was collected;
- (iv) methods to ensure accuracy, reliability, relevance, completeness, and timeliness of information should be instituted;
- (v) individuals should be notified (in advance of the collection of information) whether the furnishing of information is mandatory or voluntary, what recordkeeping practices exist, and what the uses will be made of the information; and
- (vi) individuals should be permitted to inspect and correct information concerning themselves.

Gostin et al., *supra* note 31, at 25. These principles, however, are not without cost in other areas, such as the flow of information available for administration of government programs, medical research, public health purposes, and effective law enforcement.

Providers and payors should be required to disclose to patients, in writing, how information will be used and to explain to patients their rights to limit disclosure.³¹⁶ The provider or payor should also keep a record of all disclosures and share this with the patient upon request.³¹⁷ Patients should be able to examine, copy, and propose corrections to their records.³¹⁸ However, the proposal exempts service organizations from the obligation to provide patient access and accept corrections because of the lack of privity and direct contact.³¹⁹

All of the current congressional proposals follow the Secretary's model and allow patients to inspect and copy their medical records, submit corrections and amendments, and require the disclosing party to maintain a record of all disclosures, which is to be shared with the patient upon request.³²⁰ The McDermott bill follows the Secretary's model most closely by not requiring the agents or contractors of the health information trustee to accede to patient requests to inspect or copy the medical records held by these third parties.³²¹ Furthermore, such third parties will not be permitted to correct medical records received from a trustee.³²² The Leahy bill follows the model of credit bureau laws in allowing the individual to submit a supplement to the medical record (including any corrections), rather than allowing direct corrections of the record.³²³ The Condit bill adds a further requirement: at the request of the individual, the trustee shall make reasonable efforts to inform known sources of corrections to the record.³²⁴

All of these approaches to consumer control of individual medical records would improve on current patient access. Currently, only twenty-eight states even allow patients access to their medical records.³²⁵ Provided that more favorable state access laws

316. See SHALALA REPORT, *supra* note 1, § I(G).

317. See *id.*

318. See *id.*

319. See *id.* § II(A)(4). Patients are expected to contact their providers or payors, who may by contract require action by the service organizations. See *id.*

320. See H.R. 1815, 105th Cong. §§ 101–103 (1997); H.R. 52, 105th Cong. §§ 101–104 (1997); S. 1368, 105th Cong. §§ 101–103 (1997).

321. See H.R. 1815, § 101(h).

322. See H.R. 1815, § 102(f).

323. See S. 1368, § 102(a).

324. See H.R. 52, § 102(a)(1)(D).

325. See *Medical Records Privacy: Hearings Before the Senate Comm. on Labor and Human Resources*, 105th Cong. (Oct. 28, 1997) (opening statement of Sen. Bob Bennett), available in CONGTMY, 1997 WL 14152618 [hereinafter Bennett State-

would not be pre-empted, any of the variations noted above would appear acceptable.

4. *Informed Consent*

Under the Secretary's recommendations, health care providers, payors, and their contracted services organizations would not need to obtain the patient's informed consent to collect and use patient data.³²⁶ The use of the information would be limited to "purposes compatible with and directly related to the purposes for which the information was collected or received."³²⁷ The traditional patient informed consent for disclosure would be replaced with comprehensive statutory controls on use and disclosure of information by providers and payors.³²⁸

The AMA position supports the patient's right to give or withhold informed consent for each disclosure.³²⁹ A patient's first consent should not be treated as a blanket authorization that automatically applies to all subsequent disclosures.³³⁰ According to the AMA, secondary disclosures of individually-identifiable records should be prohibited without subsequent authorization.³³¹ In addition, requests for records should specify the portion of the records needed, the time period of the records needed and the purpose of the request.³³² Based on these principles, the AMA concludes that the Secretary's proposals are "incompatible with the rights of the patient . . . because little attention is paid to the all-important issue of patient consent."³³³ The AMA criticizes the Secretary's proposal because it includes a presumption of patient consent for disclosures for health care and payment purposes (giving the patient only the opportunity to object), which if broadly construed could lead to improper unauthorized disclosures.³³⁴ The AMA is con-

ment].

326. See SHALALA REPORT, *supra* note 1, § II(A)(1).

327. *Id.* § II(B)(1).

328. See *id.* § II(E)(1).

329. See AMA Statement, *supra* note 310; AMA Editorial, *supra* note 310; MMS Policy, *supra* note 310.

330. See AMA Statement, *supra* note 310; AMA Editorial, *supra* note 310; MMS Policy, *supra* note 310.

331. See AMA Statement, *supra* note 310; AMA Editorial, *supra* note 310; MMS Policy, *supra* note 310.

332. See AMA Statement, *supra* note 310; MMS Policy, *supra* note 310.

333. AMA Editorial, *supra* note 310.

334. See AMA Statement, *supra* note 310.

cerned that too many activities will be categorized as “payment or treatment” purposes, when they may be only indirectly related to payment or the patient’s treatment.³³⁵

Senator Leahy’s bill would require individual patient authorizations virtually every time medical information is transferred.³³⁶ Health industry groups have expressed concern that such a stringent limitation on the movement of information, even within an integrated health system, could impede quality assurance, utilization review, quality improvement, disease management and related research.³³⁷ In this situation, if the balance tips too far in the direction of individual privacy, the individual’s own health care can be impeded. The legislation proposed by Representative Condit strikes a better balance in that it would allow a health information trustee to disclose protected health information for the purposes of providing health care, payment for health care, licensing and accreditation, and the utilization and qualitative assessments of providers.³³⁸

Informed consent is a key aspect of fair information practices. Individuals should have a right to know about and approve the uses of their confidential medical information. Explicit, voluntary consent of the individual should be required for disclosure; nevertheless, secondary disclosures should be allowed without separate consent in certain circumstances, such as for continuing health care treatment and payment for services. The patient should be informed at the time of the original authorizations of these secondary uses of the information. Furthermore, informed consent requires not only informing the individual of the intended uses of the information, but the safeguards to be provided. Informed consent should also require an explanation of the varying state and federal laws to which the data might become subject. This has obvious administrative difficulties in the absence of uniform, pre-emptive

335. *See id.*

336. *See* S. 1368, 105th Cong. § 202 (1997). Some exceptions are made, for example, in emergency situations, which pose a threat to the patient or to others. *See id.* § 211.

337. *See Medical Privacy Bills Dubbed a Threat to Quality of Care*, CONGRESS DAILY, Dec. 16, 1997, available in WESTLAW, CONGDLY, 1997 WL 16432774 (statement by the Healthcare Leadership Council); *Concerns About Federal Preemption of State Laws Debated at Senate Hearing*, BNA HEALTH CARE DAILY, Feb. 27, 1998, available in WESTLAW, BNA-NEWS, 1997 WL 6432774 (statement of a physician practicing in a nonprofit health care system).

338. *See* H.R. 52, 105th Cong. § 113 (1997).

federal legislation; nevertheless, if the information is to be transmitted to a state with lesser privacy protections, this should be disclosed. Unless the individual understands all the implications of giving consent, the consent is not truly informed.

5. *Disclosures for Public Purposes*

The Secretary's recommendations reflect an attempt to provide a balance between the social needs for disclosure and the individual's privacy.³³⁹ The Secretary concludes that while health care information should be protected, it should also be disclosed to support activities that are a national priority.³⁴⁰ For these activities, patient consent would not be required, but there should be legislative restrictions on how that information may be used or disclosed.³⁴¹ The Secretary identified four national priorities that would fall into this category: oversight of the health care system, public health, medical research, and law enforcement.³⁴²

a. *Oversight of the Health Care System*

Under the Secretary's recommendations, disclosures for oversight of the health care system would include disclosures for the purpose of qualitative review of providers by public or private entities, and disclosures to public agencies necessary for the licensing and certification of providers and investigations of fraud and abuse.³⁴³ Although, generally, entities receiving such disclosures would be limited to using that information for health care system oversight, public agencies would be permitted to use and disclose that information to the extent otherwise provided by law.³⁴⁴ This broad exception violates the fair information practices principle that information collected for one purpose should not be used for another without consent.

339. See SHALALA REPORT, *supra* note 1, § I(I).

340. See *id.*

341. See *id.* §§ II(B)(2) & II(H)(1).

342. See *id.* §§ II(E)(2), (3), (4), (9).

343. See *id.* § II(E)(2).

344. See *id.* § II(E)(2). For example, if a public agency discovered during a provider licensing review that one of the provider's patients was a user of illegal drugs, that licensing agency could turn the information over to law enforcement, if not prohibited by other government data practices legislation.

b. *Public Health*

According to the Secretary, individually-identifiable medical information needed for public health purposes should be disclosed to governmental health authorities, and those authorities should be allowed to further disclose that information, provided it is for health care, public health, research or public health oversight activities.³⁴⁵

The Leahy bill and McDermott bill both endorse disclosures to public health agencies, provided there is a specific nexus between the individual's identity and a threat of harm to an individual or to the public health, and where the disclosure of individually-identifiable medical information would prevent or the significantly reduce the risk of that harm.³⁴⁶ Thus, where individually-identifiable data is not necessary to the purpose, it cannot be disclosed.

The McDermott bill goes on to require that the public health authority may not use that information for other than public health purposes.³⁴⁷ In contrast, the Condit bill specifically addresses a concern raised by the Secretary's recommendations regarding health system oversight, but appropriate here as well—the Condit bill would prohibit the information disclosed to the public health agency from being used or disclosed “in any administrative, civil, or criminal action . . . against the individual” *unless necessary for the public health*.³⁴⁸

c. *Medical Research*

Medical research is an integral part of health care in the long term. The Secretary recognized this by designating medical research as a valid purpose for which to allow disclosures without patient consent, under certain conditions.³⁴⁹ Individual informed consent would be required unless it would make the research impracticable, provided the research has been reviewed by an institutional review board in whose judgment the research is of sufficient importance as to outweigh the intrusion into the privacy of the pa-

345. See *id.* § II(E)(3).

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

347. See H.R. 1815, § 209(c).

348. H.R. 52, § 115(b).

349. See SHALALA REPORT, *supra* note 1, § II(E)(4).

tient.³⁵⁰ The Secretary also recommends that providers and payors be allowed to disclose patient information (without authorization) to state health data systems on the same basis as disclosures for medical research.³⁵¹

On this issue, the AMA appears to be in general agreement with the Secretary. The AMA emphasizes that, *wherever possible*, medical data supplied to researchers should not be provided in individually-identifiable form, unless there is informed consent by the patient.³⁵² The AMA also accepts the concept of an institutional review board.³⁵³ Nevertheless, the AMA suggests that proposed consent exceptions for research may lead to problems. Research can include many types of projects, and researchers will understandably attempt to have their research categorized in ways to fit the broadest exceptions, with the least restrictive uses.³⁵⁴

The Condit bill follows the Secretary's model, allowing disclosure to approved medical researchers without patient authorization, provided the research would be impracticable to conduct without this information, and an institutional review board determines that the project is "of sufficient importance so as to outweigh the intrusion into the privacy of the protected individual who is the subject of the information"³⁵⁵ In contrast, the legislation proposed by Representative McDermott and by Senator Leahy would require consent of subjects before individually-identifiable health information could be disclosed to researchers.³⁵⁶

350. *See id.* These recommendations incorporate the stringent standards for medical research use of patient information that were developed by the Privacy Protection Study Commission in 1977. *See id.*

351. *See id.* § II(E)(6). These programs "collect health data for analysis in support of policy, planning, regulatory, and management functions identified by State statute or regulation." *Id.* The Minnesota Health Data Institute is an example of such an organization.

352. *See* AMA Statement, *supra* note 310; AMA Editorial, *supra* note 310; MMS Policy, *supra* note 310.

353. *See* AMA Statement, *supra* note 310.

354. *See* AMA Statement, *supra* note 310. These uses may not fit with patient expectations when they give personal information to their health care providers. *See id.* "Patients generally believe that their signature releases personal information for their direct and specific benefit; overly broad legislative definitions should not exploit patients' lack of knowledge regarding complex information systems." *Id.*

355. H.R. 52, 105th Cong. § 116(a)(3) (1997).

356. *See* H.R. 1815, 105th Cong. § 210(a)(2) (1997) (requiring patient consent for disclosure); S. 1368, 105th Cong. § 222(a) (1997) (stipulating that current federal regulations for the protection of human research subjects will continue to apply, citing the regulations to be found at 45 C.F.R. § 46.101 to .409, wherein §

Medical researchers argue that if the data protection regulations are too strong, they will substantially reduce the pace of scientific progress and quality research in health care and raise costs significantly.³⁵⁷ Some research, such as retrospective studies would become impossible if individual consent were required.³⁵⁸ Retrospective studies are important in assessing health and disease trends.³⁵⁹ Laws which prevent long-term studies of disease and treatment outcomes could adversely affect the public health.³⁶⁰ Moreover, consent requirements could strongly bias research studies, because the studies would be based only on patients who gave consent.³⁶¹ This introduces a selection bias to the research that may make the results "harmfully misleading."³⁶²

There is a scarcity of documented abuses of confidential patient information in approved medical research studies.³⁶³ This suggests that patients are unlikely to be harmed by the release of their medical records to researchers, even without specific authorization. Furthermore, the Mayo Clinic found that the vast majority of patients provided a general authorization for release of their records for research.³⁶⁴ This overwhelming level of cooperation and

46.116 requires informed consent of the subject).

357. See *Medical Records Privacy: Hearing Before the Subcomm. on Gov't Management, Info. and Tech. of the House Comm. on Gov't Reform and Oversight*, 105th Cong. (June 5, 1997) (Testimony of Elizabeth B. Andrews, Ph.D., on behalf of the Pharmaceutical Research and Manufacturers of America (PhRMA)), available in WESTLAW, USTESTIMONY, 1997 WL 297199; see also L. Joseph Melton III, *The Threat to Medical-Records Research*, 337 NEW ENG. J. MED. 1466, 1467 (1997).

358. See Andrew A. Skolnick, *Opposition to Law Officers Having Unfettered Access to Medical Records*, 279 JAMA 257, 258 (1998) (citing Melton, *supra* note 357, at 1466-69).

359. See *id.*

360. See *id.*

361. See *id.*

362. *Id.* For example, if due to the consent requirements the study excluded patients who died and patients with bad outcomes who refused to participate in follow-up, this selection bias could make even dangerous treatments appear to have beneficial outcomes. See Melton, *supra* note 357, at 1468.

363. See Melton, *supra* note 357, at 1466 (citing NATIONAL COMM. OF VITAL AND HEALTH STATISTICS, HEALTH PRIVACY AND CONFIDENTIALITY RECOMMENDATIONS (June 25, 1997)).

364. See *id.* at 1467. "As of October 1997, 96% of the 214,000 patients who returned forms have provided this general authorization for the Mayo Clinic to use their medical-records information for research if needed." *Id.* This patient authorization was required under a new Minnesota law, effective January 1, 1997, which requires providers to notify in writing all patients seeking medical care that medical records may be released for research and that the patient may object, and to obtain that patient's general authorization for the release of records for re-

agreement by patients is consistent with the Secretary's proposal of constructive consent.³⁶⁵ Therefore, the Secretary's recommendations in this area should be followed; however, "research" should not be defined so broadly as to permit the disclosure of individually-identifiable health information for marketing or commercial purposes.

d. Law Enforcement

The Secretary's final public purpose exception would be made for law enforcement.³⁶⁶ This requirement maintains the status quo, allowing broad non-authorized disclosures of medical information to aid law enforcement in investigations.³⁶⁷ Health care providers have objected to this as allowing law enforcement agents and the U.S. intelligence community "carte blanche access and use of patient information."³⁶⁸ The AMA recommends that all exceptions to the requirement for patient consent be narrowly drawn; therefore, law enforcement officials should be required to show probable cause for the non-consented release of medical data.³⁶⁹

Of the proposed legislation discussed in this article, the Leahy bill would provide the most protection to patient records. The Leahy bill would require law enforcement officials to obtain a court order to access protected patient information.³⁷⁰ Senator Bennett's bill is also more restrictive of law enforcement access to records than recommended by the Secretary.³⁷¹ Law enforcement officials would be required to obtain a subpoena or warrant, and should specify what information is sought and how it will be used.³⁷²

This law enforcement provision is one of the more controversial aspects of the Secretary's recommendations and will undoubtedly continue to stir debate. It is of particular concern because of the computerization of records.³⁷³ With all the other complexities of this legislation, the Secretary may be correct that until more ex-

search. *See id.* at 1466; *see also* MINN. STAT. § 144.335, subd. 3(a)(d) (1996).

365. *See* Melton, *supra* note 357, at 1467.

366. *See* SHALALA REPORT, *supra* note 1, § II(E)(9).

367. *See id.* § II(B)(9), (10).

368. Skolnick, *supra* note 358, at 257.

369. *See* AMA Statement, *supra* note 310; AMA Editorial, *supra* note 310.

370. *See* S. 1368, 105th Cong. § 215(a) (1997).

371. *See* S. 2609, 105th Cong. § 210 (1998); *see also* Bennett Statement, *supra* note 325.

372. *See id.*

373. *See* SHALALA REPORT, *supra* note 1, § II(E)(10).

perience is gained with the law enforcement possibilities inherent in the search capabilities of computerized medical records, it would be "premature to change existing law in this area."³⁷⁴

6. Penalties/Sanctions

The Secretary recommends that the force of law, in the form of criminal and civil penalties, should be used to enforce this new federal legislation, and the patient should also have the option of suing for actual damages and equitable relief.³⁷⁵ All of the proposed bills provide these remedies, with variations on the extent of damages or punishment, and statute of limitations for civil actions.³⁷⁶ Health care providers will undoubtedly have concerns about inadvertent, harmless disclosures. The AMA position focuses on proportionality of the penalty to the harm. That is, penalties and sanctions for improper disclosure for profit, commercial purpose or malicious purposes, should be commensurate with the harm caused to the patient; however, unintentional disclosures, where there was not demonstrable harm to the patient should invoke minor, if any, penalties.³⁷⁷

Most of the discussion on confidentiality of medical records focuses on the rights of the patient. While these rights are of obvious importance, the rights of recordkeepers must also be considered. Any health care provider or other holder of confidential records will be, and should be, accountable for following the legal requirements for maintaining the confidentiality of information. It is therefore critical for the legislation in this area to be very clear about what safeguards and procedures will be required of those gatekeepers.

7. Federal Pre-emption.

The Secretary's report recommends that the new privacy legislation not pre-empt or modify any existing state or federal laws that provide a greater degree of protection for health care information.³⁷⁸ The proposal is for a federal "floor," or minimum protec-

374. *Id.*

375. *See id.* § II(H)(1). For knowing violations, attorney fees and punitive damages would also be available. *See id.*

376. *See* H.R. 52, 105th Cong. §§ 151-154 (1997); H.R. 1815, 105th Cong. §§ 301-311 (1997); S. 1368, 105th Cong. §§ 311-323 (1997).

377. *See* AMA Statement, *supra* note 310; MMS Policy, *supra* note 310.

378. *See* SHALALA REPORT, *supra* note 1, § I(J). If either state or federal law

tions.³⁷⁹ This recommendation follows the preference expressed by Congress in enacting HIPAA.³⁸⁰

The proposed medical privacy bills take different approaches to pre-emption. The McDermott and Leahy bills are in accord with the Secretary's recommendations and do not pre-empt any existing state laws offering the patient better access to records or more protection from disclosure (whether based in statute or common law).³⁸¹ In contrast, the Condit bill does pre-empt state medical privacy laws, with the exception of state laws regarding public health and mental health records, and government data practices acts.³⁸² Taking the strongest position on pre-emption, Senator Bennett's bill favors full pre-emption of state medical records laws.³⁸³ The Kansas commissioner of insurance, Kathleen Sibelius, testifying before Congress, opined that this broad language is too sweeping and may cause unintended consequences in several states.³⁸⁴ The AMA raises another concern about federal pre-emption of state laws—the standard may not be set high enough at the federal level.³⁸⁵

Federal preemption of state laws is controversial, because if the federal statute is weaker than some state statutes, the result would be a decrease in protection in those states. However, as a long-term strategy, state-by-state regulation of privacy is not compatible with modern methods of health care finance and delivery.³⁸⁶ Lack of

prohibited disclosure, no disclosure would be allowed. Furthermore, the proposal does not envision treating different types of health care information differently; the same protections are afforded HIV status, mental health records, and all other medical records held or disseminated by providers or payors. *See id.* § I(K). Although certain types of sensitive information deserve special protections, this can be accomplished by not pre-empting existing higher standards for protecting that information. *See id.* This should alleviate some of the practical difficulties for health care providers who are treating patients for more than one condition, each of which has different rules regarding confidentiality of the records. *See generally* Skolnick, *supra* note 358.

379. SHALALA REPORT, *supra* note 1, § I(K).

380. *See id.* § I(K) (citing HIPAA provisions).

381. *See* H.R. 1815 § 402(a); S. 1368 § 401(a); *see also* SHALALA REPORT, *supra* note 1, § 1(J).

382. *See* H.R. 52, 105th Cong. § 304 (1997).

383. *See* S. 2609, 105th Cong. § 401 (1998); *see also* Bennett Statement, *supra* note 325.

384. *See Concerns About Federal Preemption of State Laws Debated at Senate Hearing*, BNA HEALTH CARE DAILY, Feb. 27, 1998, available in WESTLAW, BNA-HCD, 2/27/98 BNA-HCD d7, 1997 WL 16432774 (testimony before Senate Comm. Labor & Human Resources on medical records privacy).

385. *See* AMA Statement, *supra* note 310; MMS Policy, *supra* note 310.

386. *See* Gostin, *supra* note 131, at 516. Medical data commonly flows outside

uniformity of privacy protections may also impair a patient's ability to make meaningful consent to disclosure because of failure to understand which regulations apply and may undermine efforts to automate health care information.³⁸⁷ Nevertheless, due to the complexity of enacting a federal medical privacy law, it would be best to retain stronger state protections, at least in the interim, to avoid unintended consequences which sacrifice patient rights.

8. Summary

The number of bills introduced in Congress, and the extent of criticisms of those bills, are indications of the complexity of the task. There is a need to balance the privacy needs of the individual and the public's need for disclosure, such as for public health and research purposes. In addition, there are a great many different interest groups with a stake in such legislation. As a result, designing workable (and enact-able) medical data privacy legislation continues to challenge lawmakers.

X. CONCLUSION

As technology continues to advance and computerized databases designed to access, analyze and disseminate vast amounts of health care information proliferate, the risks of public disclosure of this data continues to increase. A balance must be struck between the protection of individual privacy and the need for disclosure for the common good. The current patchwork of federal and state laws provides insufficient protection to individually-identifiable medical data. Uniform federal legislation, which supersedes weaker state laws, will be necessary to provide reliable protection and smooth interstate transfer of information. Although the Health Insurance Portability and Accountability Act raises new privacy concerns, it can also be the vehicle for providing the crucial federal standards.

the state where it originated, for example, to third-party payors or for research purposes. *See id.* The physical location of the medical data is no longer relevant in the electronic age, and use of information will not be restricted to the state in which it is created. *See id.* Regulating information based on the state in which it is first generated would cause confusion as to which state laws govern as data is transferred across state lines. *See id.*

387. *See id.*

A number of privacy bills have been proposed in Congress, and these matters will continue to be debated. Because of the various interest groups with a stake in the outcome, and the need for a careful balancing of public and private interests, it may prove very difficult for Congress to pass privacy legislation. If the health care industry believes the legislation will be too costly to implement; if researchers and public health agencies believe the provisions will handicap their efforts; if privacy advocates believe that the legislation only maintains the status quo or erodes protections in certain areas; there may be a stalemate. In that case, HIPAA requires the Secretary of Health and Human Services to promulgate privacy regulations; however, the path for rulemaking may not be much smoother than for legislation.