UIC John Marshall Journal of Information Technology & Privacy Law

Volume 12
Issue 4 *Journal of Computer & Information Law - Spring 1994*

Article 4

Spring 1994

The American Health Security Act and Privacy: What Does It Really Cost?, 12 J. Marshall J. Computer & Info. L. 585 (1994)

Susan E. Corsey

COMMENTS

THE AMERICAN HEALTH SECURITY ACT AND PRIVACY: WHAT DOES IT REALLY COST?

I.INTRODUCTION

For months, millions of Americans anxiously awaited the unveiling of President Clinton's proposed reform of the nation's health care system. On September 22, 1993, President Clinton addressed a joint session of Congress and presented his health care proposal known as the "American Health Security Act" (Act).[1] Under the Act, comprehensive health care insurance[2] is guaranteed to all Americans[3] regardless of their health[4] or employment status.[5] This would provide health insurance for thirty-seven million Americans who are presently without coverage.[6]

---

1. *Clinton Administration Description of President's Health Care Reform Plan, "American Health Security Act of 1993,"* 1993 Daily Labor Report Special Supplement (BNA) No. 175 (Sept. 7, 1993) [hereinafter *American Health Security Act*].

2. The Act guarantees a comprehensive benefit package with no lifetime limits on medical coverage. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 1001(b) (1993). Health insurance is designed to protect the consumer from financial loss due to illness or injury. JO ANNE CZECOWSKI BRUCE, PRIVACY AND CONFIDENTIALITY OF HEALTH CARE INFORMATION 195 (Marcia Bottoms ed., 2d ed. 1988).

3. The Act will provide health care coverage for all American citizens, legal residents, and long term non-immigrants. Dan Goodgame, *Clinton's Health Plan*, TIME, Sept. 20, 1993, at 54, 57. Undocumented persons will not be eligible for health benefits under the Act. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 1005(a) (1993).

4. A preexisting condition is an "injury, disease, or other physical condition that exists prior to the issuance of a health insurance policy" for which a provider denies benefits. BRUCE, *supra* note 2, at 197. The Act prohibits health plans from denying enrollment or charging higher fees for patients because of age, medical condition, or other factors related to risk. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 11004(b)(3)(B)(ii) (1993).

5. *American Health Security Act, supra* note 1, at S-3. Government polls reveal that many Americans fear that they will lose their health insurance due to layoffs or cutbacks on insurance. Goodgame, *supra* note 3, at 55. A health plan cannot cancel an enrollment until the individual enrolls in another plan. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 1323(g) (1993).

6. *American Health Security Act, supra* note 1, at S-2. Experts estimate that one out of four or 63 million people will be without health care coverage for at least some time

In 1991, the health care industry spent an estimated 100 to 240 billion dollars on the administration of a redundant paper-based system.[7] A crucial feature of Clinton's proposal is a nationwide electronic data system, which is capable of managing tremendous amounts of patient information.[8] The computerized system will streamline information[9] and cut expenses.[10] Still, this advanced technology raises serious issues concerning the confidentiality[11] of patient information and medical records.[12]

This Comment discusses the Act's dependence on the electronic collection and dissemination of patient health care information, and the

---

before 1995. *Id.* Eighty-five percent of Americans without health insurance are employed workers with dependents. Goodgame, *supra* note 3, at 55.

7. Terri Finkbine Arnold, Note, *Let Technology Counteract Technology: Protecting the Medical Record in the Computer Age*, 15 HASTINGS COMM. & ENT. L. J. 455, 467 (1993). The Act will alleviate the unnecessary administrative paperwork such as regulatory, billing, and reporting requirements, which presently overburden the health care provider. *American Health Security Act*, *supra* note 1, at S-4. The Act proposes standard forms for insurance reimbursement, claims, and clinical encounter records. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5130(a) (1993). In turn, the medical personnel can spend their time more efficiently by focusing on providing high-quality care. *American Health Security Act*, *supra* note 1, at S-3.

8. *American Health Security Act*, *supra* note 1, at S-35. The electronic network will contain enrollment, financial, and encounter data. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5101(e) (1993). The National Health Board must develop and implement a health information system within two years of the Act's enactment. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5101(a) (1993). The advanced technology in personal computers, networks, and database retrieval tools facilitate the management of large amounts of patient data, which can be accessed in a physician's office or throughout the country. Arnold, *supra* note 7, at 458-59. Computers have the capability to collect, store, retrieve, process, and disseminate information, which "threatens individual privacy in ways that were unimaginable just a short time ago." Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395 (1987).

9. The Act proposes to streamline information by using standard forms, uniform health data sets, electronic networks and national standards for electronic data transmission. *American Health Security Act*, *supra* note 1, at S-35.

10. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5101(c) (1993). Health care costs are the fastest growing expense in the present economy. *American Health Security Act*, *supra* note 1, at S-3. The Act proposes to bring growth in health care costs in line with growth in Gross Domestic Product by 1997, through increasing competition, reducing administrative costs and imposing budget disciplines. *Id.*

11. Confidentiality is the treatment of personal information as "private and not for publication." BLACK'S LAW DICTIONARY 298 (6th ed. 1990). The Act includes a policy of protecting patient privacy and confidentiality. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5120(a) (1993).

12. The medical record is created by the health care institution and is a compilation of information regarding the care and services delivered to a patient. Bruce, *supra* note 2, at 196. The medical record is comprised of a patient's intimate health care information, including medical history, clinical treatment, administrative, and financial resources. Arnold, *supra* note 7, at 457.

threat it poses to the individual's constitutional right to privacy. Section II of this Comment offers a brief overview of the computer related aspects of the Act. Section III analyzes a patient's legal right to privacy in tort and constitutional law, and explores possible remedies. Section IV explores a patient's right to protect the privacy of his or her medical records. Finally, Section V discusses the court's response to computerized medical information and the Act's potential for intrusion into a patient's privacy. It also proposes security measures to protect the confidentiality of medical information.

Everyone has a fear of that inevitable moment in life, when you see your life flash before your eyes. Thanks to the electronic storage of medical information, your life can flash before someone else's eyes. With the Act's dependence on a computerized information system, the patient will find his or her entire personal, medical, and financial history consolidated into one "womb-to-tomb dossier."[13] Just imagine every intimate detail of your abortion, HIV status, high school drug problem, or suicide attempt easily accessible for the viewing of another.

The Act's potential for unwarranted disclosure of intimate medical information threatens the constitutional right to privacy of every American who utilizes the health care system. Only the legislature has the authority to enact protection for the privacy of all Americans. Therefore, Congress must standardize security measures for computerized health care information to protect patients' constitutional privacy interest.

II. COMPUTER FEATURES OF THE HEALTH SECURITY ACT

President Clinton's proposed reform of the nation's health care system promises continued health care coverage for every American, regardless of employment status or illness.[14] Clinton's goal is to maintain consumer choice[15] and provide high-quality health benefits, while con-

13. Arthur R. Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUM. RTS. L. REV. 1, 3 (1972) (identification number given at birth could become a way to monitor an individual throughout his or her life). The person controlling computerized personal information has a degree of power over the individual, who is subject to abuse. *Id.*

14. *See supra* notes 4-5.

15. Consumers will continue to have several insurance plans to choose from. Goodgame, *supra* note 3, at 56. The consumer can seek treatment with an individual doctor in the fee-for-service plan, which will be the most costly. *Id.* The Preferred Provider Organization (PPO) requires the patient to go to a specific doctor and hospital. *Id.* The most affordable plan is the Health Maintenance Organization (HMO), which provides health care for a fixed price. *Id.* President Clinton decided not to mandate a "single-payor health insurance (Canadian) model" since it does not allow consumers the choice between health plans. Deborah Cunningham Foshee & Judith W. Giorlando, *Health Care Reform: A Primer*, HEALTH LINK, Summer 1993, at 1.

trolling rising health care costs.[16] In order to comply with the Act, a health plan must meet national standards on benefits, quality, and access to care.[17] At the same time, each individual state will have the autonomy to develop a plan which best suits its needs.[18]

The key element of Clinton's health care plan is a completely automated information system.[19] The most basic source of information is the health security card,[20] which is much like an ATM card.[21] Every American will receive a card which provides access to health care services anywhere within the United States.[22]

Clinton proposes a new framework[23] for health care information.[24]

---

16. Foshee & Giorlando, *supra* note 15, at 1. If left unregulated, health care costs are predicted to reach 16% to 18% of the gross domestic product by the year 2000. *Id.*

17. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5001 (1993). The National Health Board will develop and implement standards related to eligibility of individuals for coverage. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 1503(c) (1993). The National Quality Management Council will develop and implement standards for evaluating the clinical appropriateness of protocols used to manage health services utilization. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5006(a)(3) (1993).

18. *American Health Security Act*, *supra* note 1, at S-3. Many rural areas are expected to adopt a "single-payer" system, where the state utilizes tax revenues to pay for its residents' health care costs. Goodgame, *supra* note 3, at 56. The states will evaluate a health plan's quality, financial stability, and capabilities. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 1203(a)(2) (1993). Each state is allowed flexibility in its choices of health care plans. Goodgame, *supra* note 3, at 56. The states will be responsible for ensuring that all eligible individuals have access to health care coverage. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 1203(e)(1)(A)(i) (1993).

19. *American Health Security Act*, *supra* note 1, at S-35.

20. The health security card will include information regarding the identity of the individual, the health plan, the policy, and any other information the National Health Board determines necessary. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5105(b) (1993). For the protection of privacy, the Act will utilize unique individual identifiers by issuing a number created specifically for the health care system. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5104 (1993). The national privacy policy prohibits the connection of health care information with the identification number. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5104(b) (1993).

21. United States v. Camacho, 998 F.2d 1010 (4th Cir. 1993). The Automatic Teller Machine (ATM) card allows a customer to withdraw cash from his or her account electronically. *Id.* To access the account, the customer inserts the card into an ATM and enters the Personal Identification Number (PIN) for that card. *Id.*

22. *American Health Security Act*, *supra* note 1, at S-35.

23. The information framework will be responsible for maintaining the health security cards, streamlining administrative activities, and providing consumer information. *Id.* The information framework will develop a link between medical records to enhance the quality of care. *Id.*

24. *American Health Security Act*, *supra* note 1, at S-35. Health care information includes data on enrollment, clinical encounters, utilization management, payment of benefits, administration, finances, grievances, characteristics of regional and corporate alliances, information from the National Health Board, and terms of agreement between

This framework involves "standard forms,[25] uniform health data sets[26], electronic networks,[27] and national standards for electronic transmission."[28] This consolidation of patient information fosters greater efficiency, but at the same time jeopardizes patient confidentiality.

As part of the automated system, each encounter with a health care provider[29] is documented electronically and transmitted to a national network.[30] The ultimate goal is to have an electronic "point-of-service"[31] information system, which provides clinical, administrative, and financial data to "employers, health plans, physician's offices, hospitals, laboratories, pharmacies, and other providers."[32] The new health care system will establish an electronic network of federal, state, and alliance[33] regional centers.[34] This network will consist of enrollment,[35] fi-

---

the health plans and the providers. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5101(e) (1993).

25. When electronic form is not specified by the National Health Board, the Act requires uniform paper forms containing standard data elements, definitions, and instructions for completion. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5102(b)(1) (1993). The National Health Board will develop, promulgate, and publish standard health care benefit forms for enrollment, disenrollment, clinical encounters, and claims within one year of the Act's enactment. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5130(a) (1993). Standard claim forms will be implemented by health plans as of January, 1995. Goodgame, *supra* note 3, at 57.

26. The Act proposes uniform health data sets which utilize routine definitions to standardize the collection and transmission of data in electronic form. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5102(b)(2) (1993).

27. The electronic data network will consist of regional centers that collect and transmit information. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5103(a) (1993). The information system will provide an avenue for the analysis of a patient's physical status and health trends, in addition to an evaluation of the health care system. *American Health Security Act*, *supra* note 1, at S-35.

28. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5101(a) (1993). The Act proposes the development of requirements for electronic data interchange among automated health information systems. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5102(b)(4) (1993).

29. A health care provider is usually a doctor, nurse or allied health care worker, who supplies health care services in return for financial reimbursement for the cost in rendering the services. BRUCE, *supra* note 2, at 197.

30. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5101(e)(2) (1993). The electronic capture, retention, and transmission of the encounter record must become part of the provision of care. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5106(2) (1993).

31. The point-of-service information system provides important information to consumers, health care providers, payers and policy makers, which fosters continuing quality improvement. *American Health Security Act*, *supra* note 1, at S-36.

32. *American Health Security Act*, *supra* note 1, at S-36. The Act proposes federal guidelines for the protection of confidentiality of all records submitted to health alliances. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5120(a) (1993).

33. Alliances are a coalition of health insurance buyers that bargain with competing networks of health care providers for the best coverage and rates for small employers and individuals. Goodgame, *supra* note 3, at 55. Employers with 5000 or fewer employees will be part of a regional alliance. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 1311(b)(1)(B)(ii)

nancial, and utilization data.[36]

The Act recognizes the need for additional security measures for the protection of privacy[37] and proposes the development of uniform national standards for the protection of individually identifiable[38] health care information.[39] This standard would protect all types of records, including paper, microfilm, or electronic data.[40] Yet, these proposals are misleading. The Act fails to address specific standards for security and does not mandate the development and implementation of security standards until years after the Act's enactment.[41] Before addressing the necessity of additional security measures for the protection of privacy, it is important to consider whether a patient has a right to privacy in his or her medical record.

III. AN INDIVIDUAL'S RIGHT TO PRIVACY

Society has placed conflicting demands on the health care industry, calling for "inexpensive high-quality medical care,[42] administrative effi-

(1993). Employers with more than 5000 employees will establish a corporate alliance. *Id.* Alliances shall begin as early as 1995 and will be mandatory as of January 1997. Goodgame, *supra* note 3, at 57.

34. *American Health Security Act*, *supra* note 1, at S-37. As long as it remains within the realm of the national uniform standards, the health plans and alliances are allowed to collect data and patient information according to its needs. *Id.* at S-36.

35. Enrollment data is information used to record or register an applicant. BLACK'S LAW DICTIONARY 530 (6th ed. 1990).

36. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5101(e) (1993). The network allows analysis of budgets, access, and state accountability. *Id.*

37. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5120(a) (1993).

38. Individually identifiable information "establishes the identity of a specific patient." BRUCE, *supra* note 2, at 197. Individually identifiable health information is any information that relates to the health, payment, or provision of care which can be readily associated with the identity of the individual enrolled. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5123(3) (1993).

39. *American Health Security Act*, *supra* note 1, at S-39. The health information system will include a unique identifier number for each individual, employer, health plan, and provider. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5104(a) (1993). The system promises privacy, confidentiality and security protection, through "national standards for clinical and administrative data." *American Health Security Act*, *supra* note 1, at S-35.

40. *American Health Security Act*, *supra* note 1, at S-39.

41. Within two years of the Act's enactment, the National Health Board will develop standards to protect the privacy of individually identifiable health information as well as safeguards for the security of information contained in the information system. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5120(a) (1993). Within three years of the Act's enactment, the Board must submit to the President and Congress proposed legislation for Federal privacy protection of individually identifiable health information. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5122(a) (1993). The Board will oversee the establishment and administration of the new health plan by the states. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5120(a) (1993).

42. The Act proposes to improve the quality of health care through standards for

ciency, continued research,[43] and individual privacy."[44] In order to meet these demands, the utilization of personal information will be greater than ever and invasion of privacy claims will inevitably skyrocket. Invasion of privacy actions are based on tort or constitutional law. It is important to distinguish between the two claims, because each has a different burden of proof and separate remedy at law.

A. TORT CLAIM FOR INVASION OF PRIVACY

A person can be held liable in tort for the invasion of another's privacy.[45] The four tort claims for invasion of privacy are intrusion upon seclusion,[46] appropriation of name or likeness,[47] publicity given to private life,[48] and publicity placing another in a false light.[49]

---

practitioners, measuring outcomes, increased medical research and promoting primary and preventative care. *American Health Security Act, supra* note 1, at S-4.

43. The Act includes coverage for medical care provided as part of an approved research study. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 1544 (1993). The National Institute for Occupational Safety and Health sought employee medical information to utilize in a research study for the development of occupational health and safety standards. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 572 (3d Cir. 1980) [hereinafter *Westinghouse*]. The court held that although medical records are entitled to privacy protection, the interest in occupational health and safety was a substantial and justified intrusion into private information. *Id.* at 579.

44. Arnold, *supra* note 7, at 481.

45. RESTATEMENT (SECOND) OF TORTS § 652A(1) (1977).

46. Faison v. Parker, 823 F.Supp. 1198, 1205 (E.D. Pa. 1993). Intrusion upon seclusion is the intentional intrusion into the solitude, seclusion, private affairs or concerns of another, which would be highly offensive to a reasonable person. RESTATEMENT (SECOND) OF TORTS § 652B (1977). Intrusion is important in computer related litigation because it extends beyond physical intrusion and includes the mere examination of personal records. Beth Hahn Gerwin, Note, *Computer Related Litigation Using Tort Concepts*, 9 AM. J. TRIAL ADVOC. 97, 116 (1985).

47. *Faison*, 823 F. Supp. at 1205. A person is liable for invasion of privacy when he or she appropriates the name or likeness of another to his or her own use or benefit. RESTATEMENT (SECOND) OF TORTS § 652C (1977).

48. *Faison*, 823 F. Supp. at 1205. One can be liable for invasion of privacy when he or she publicizes a matter related to the private life of another, if the publicized matter "(a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." RESTATEMENT (SECOND) OF TORTS § 652D (1977). A patient claimed invasion of privacy for the publication of private matters when her pregnancy test results were revealed to her family. Martin v. Baehler, No. 91C-11-008, 1993 WL 258843, at *1 (Del. Super. Ct. May 20, 1993). The court held that the communication to family members was private and did not constitute an invasion of privacy since the information was not certain to reach the public. *Id.* at *2. Publication of private matters can be applied in computer related litigation. Gerwin, *supra* note 52, at 116.

49. *Faison*, 823 F. Supp. at 1205. Publicity which portrays another in a false light constitutes an invasion of privacy when the matter is highly offensive to a reasonable person, and the act is performed with knowledge of or in reckless disregard of the matters falsity, and the false light in which it portrays the other. RESTATEMENT (SECOND) OF TORTS § 652E (1977).

Disclosure of confidential medical records implicates the tort of publicity given to the private life of another.[50] In order to succeed, the plaintiff has the extremely difficult burden of proving the publicity element.[51] Publicity involves the communication of a private fact to more than a single person or small group.[52] The tort remedy for invasion of privacy is damages. The damages claimed are usually harm to the privacy interest, mental distress, and special damages.[53]

Even if an individual can successfully prove invasion of privacy, the courts utilize a balancing test, which weighs the need for disclosure of the information against the individual's right to privacy.[54] Thus, a person bringing a claim for invasion of privacy based on tort has multiple hurdles to overcome before he or she can recover damages. Consequently, a party may choose to seek an alternative remedy, such as an injunction.

B. CONSTITUTIONAL RIGHT TO PRIVACY

In an action for invasion of privacy under constitutional law, the party will usually seek to protect his or her privacy interest through injunctive relief.[55] The constitutional right to privacy is a relatively

---

50. *Faison*, 823 F. Supp. at 1205. An inmate claimed publicity was given to her private life, when medical and mental health information was disclosed in her presentence report, which was dispersed to various participants in the court proceedings. *Id.* The court held that the plaintiff did not have a cause of action because the disclosure was not made to the general public. *Id.* at 1206.

51. G. Michael Harvey, Comment, *Confidentiality: A Measured Response to the Failure of Privacy*, 140 U. PA. L. REV. 2385, 2441 (1992). The publicity element was created in an attempt to exempt from liability isolated, discrete breaches of confidence, such as gossip, and avoid a flood of litigation. *Id.*

52. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1977). Publicity involves communicating a matter "to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." *Id.* The disclosure of confidential information to family members did not satisfy the publicity element for invasion of privacy because it was not certain to reach the public. *Martin*, 1993 WL 258843 at *2. A report containing medical and mental health information which was contained in numerous files and typed in a typing pool did not constitute publicity because the disclosure was not made to the general public. *Faison*, 823 F. Supp. at 1206.

53. RESTATEMENT (SECOND) OF TORTS § 652H (1977). Special damages are the actual damages which are causally related to the plaintiff's injury. BLACK'S LAW DICTIONARY 392 (6th ed. 1990).

54. Jo Ellen Smith Psychiatric Hosp. v. Harrell, 546 So.2d 886, 888 (La. Ct. App. 1989). The court applied a balancing test where a hospital inadvertently released the insurance payment records of 38 former patients of a psychiatric, drug and alcohol rehabilitation facility to the parents of another patient. *Id.* The court held that the privacy interest of the 38 patients was more compelling than the defendant's right to investigate the possibility of a claim against the hospital. *Id.*

55. Peninsula Counseling Center v. Rahm, 719 P.2d 926 (Wash. 1986) (en banc). Three mental health centers brought a lawsuit seeking an injunction to prevent the De-

young concept for American courts. Justice Brandeis' famous dissent in *Olmstead v. United States*[56] first addressed "the right to be let alone." However, it wasn't until 1965 that the United States Supreme Court guaranteed the constitutional right to privacy[57] in *Griswold v. Connecticut*.[58] Even though the United States Constitution lacks an explicit reference,[59] the Supreme Court recognized the necessity of an individual's right to privacy.[60] As a result, the Court held that the right to privacy was implicit in certain penumbras[61] in the Bill of Rights, which create "zones of privacy."[62]

In spite of the right to privacy, unauthorized disclosure of personal information is permissible when it meets a valid governmental interest.[63] Thus, a party seeking an injunction to protect his or her constitutional right to privacy may be defeated by a valid governmental interest

---

partment of Social and Health Services from enforcing a system of tracking patients. *Id.* at 927-28. The court denied the injunction because the governmental interest in disclosure outweighed the individual interest in privacy. *Id.* at 929-30.

56. 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

57. The legal right to privacy has been defined as "an autonomy or control over intimacies of personal liberty." GEORGE B. TRUBOW, PRIVACY LAW AND PRACTICE, ¶ 19.01, at 19-3 (1991) (quoting Professor Gerety, 12 HARV. C.R.-C.L. L. REV. 233, 366 (1977)).

58. 381 U.S. 479, 484 (1965). The court held that a statute forbidding the use of contraceptives was unconstitutional because it violated the Due Process Clause of the Fourteenth Amendment. *Id.* The *Griswold* court quoted the well known principle "governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by the means which sweep unnecessarily broadly and thereby invade the area of protected freedoms." *Id.* at 485 (quoting NAACP v. Alabama, 377 U.S. 288, 307).

59. TRUBOW, *supra* note 65, at 19-3.

60. *Griswold*, 381 U.S. at 484.

61. Penumbras are implied powers of the Federal Government. BLACK'S LAW DICTIONARY 1135 (6th ed. 1990). The First Amendment contains the right of association. *Griswold*, 381 U.S. at 484. The Third Amendment prohibits "the quartering of soldiers 'in any house' in time of peace without the consent of the owner." *Id.* The Fourth Amendment asserts the "right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." *Id.* The Fifth Amendment prohibits the government from forcing the citizen to incriminate himself. *Id.* The Ninth Amendment provides: "The enumeration in the Constitution of certain rights, shall not be construed to deny or disparage others retained by the people." *Id.*

62. *Griswold*, 381 U.S. at 484. The recognized "zones of privacy" are the right to be free from governmental surveillance and intrusion in private affairs, the right not to have one's private life publicized by the government, and the right to be free in "action, thought, experience, and belief from governmental compulsion." Philip B. Kurland, *The Private I*, U. CHI. MAG. 7, 8 (Autumn 1976), *quoted in* Whalen v. Roe, 429 U.S. 589, 600, n.24 (1977).

63. Peninsula Counseling Center v. Rahm, 719 P.2d 926, 929 (Wash. 1986). Department of Social and Health Services sought the names and diagnosis of mental health patients, which participate in any mental health program. *Id.* at 927-28. The court held that the disclosure was permissible to meet a valid governmental interest in maintaining adequate mental health facilities and ensuring care for patients. *Id.* at 929-30.

in disclosure of the information.[64] Although an individual has a right to privacy, it is important to consider whether a patient has a right to privacy in his or her medical record.

IV. PROTECTION OF THE MEDICAL RECORD

The Act proposes to electronically document each encounter with a health care provider, which will be transmitted to a national network.[65] The electronic collection, storage, and dissemination of medical information raises the issue whether a patient has a right to privacy in his or her medical record. A patient's right to privacy was first recognized in *DeMay v. Roberts*,[66] which protected a patient from the presence of an unauthorized person during medical treatment.[67] Yet, the courts have been slow to extend this protection to the unauthorized disclosure of medical information.

In *Whalen v. Roe* the United States Supreme Court addressed the constitutional issues that arise when the government has access to patient information.[68] The Court recognized a constitutionally protected privacy interest in "avoiding disclosure of personal matters and . . . independence in making certain decisions."[69] Subsequent courts have extended this constitutional privacy interest to protect patients from disclosure of their medical records.[70] Nevertheless, the courts unequiv-

64. *See* Whalen v. Roe, 429 U.S. 589, 602 (1977) (disclosure of personal information to state permissible to protect the health of the community); and United States v. Westinghouse Elec. Corp., 638 F.2d 570, 580 (3d Cir. 1980) (public interest in facilitating research and investigation justified minimal intrusion into medical records).

65. *American Health Security Act, supra* note 1, at S-36.

66. DeMay v. Roberts, 9 N.W. 146, 149 (Mich. 1881).

67. *Id.* In *DeMay*, a physician delivered a baby in the mother's home. *Id.*. The doctor asked a nonmedical friend to go with him to the home and carry his supplies. *Id.* The friend, at the doctors request, held the mothers hand during the delivery. *Id.* When the mother learned that the friend was not a doctor or medical student, she sued the doctor. *Id.* The Michigan Supreme Court held that the mother's consent to the presence of the friend was based on an incorrect assumption that the man was part of the medical profession. *Id.* As a result, the court recognized a patient's right to privacy from the presence of an unauthorized person. *Id.*

68. *Whalen*, 429 U.S. at 602. In *Whalen*, the court addressed whether a state can maintain a record of the names and addresses of all persons who have obtained certain prescription drugs. *Id.* at 591. The record was to be stored in a centralized computer file, which was to be maintained for five years and protected by multiple security measures. *Id.* at 593-94. The court held that the patient identification requirement was a reasonable exercise of the states broad police power. *Id.* at 597-98.

69. *Id.* at 599-600.

70. United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980); *See also* Mann v. University of Cincinnati, 824 F.Supp. 1190, 1197 (S.D. Ohio 1993) (found constitutional right to privacy in medical records preventing discovery). The medical record is entitled to privacy protection, because it contains "intimate facts of a personal nature." *Westinghouse*, 638 F.2d at 577. Medical records containing reports regarding the physical

ocally reject any absolute right to confidentiality of medical information, acknowledging the necessity for certain disclosures.[71]

The measure for intrusion into a patient's private medical record is the balance between the individual's right to privacy and the government's interest in disclosure.[72] If disclosure of medical information is necessary, the disclosure must be no more than is reasonably necessary.[73] Hence, medical records are protected from unauthorized disclosure, unless there is a governmental interest in the disclosure.[74]

A. PHYSICIAN-PATIENT PRIVILEGE AS PROTECTION OF THE MEDICAL RECORD

One method for protecting the confidentiality of the medical record is through the physician-patient privilege.[75] The physician-patient privi-

---

and mental condition of a party require a higher burden for discovery than general discovery. *Id.*

71. *Whalen*, 429 U.S. at 600. An integral part of health care today requires the disclosure of "private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies." *Id.* at 602. A state may require disclosure of medical information to protect the public health, which does not amount to an impermissible invasion of privacy. *Id.* Minimal intrusion into medical records is justified when there is a public interest in research and investigation. *Westinghouse*, 638 F.2d at 580. The remote possibility that stored information will be disclosed inappropriately is not sufficient reason for invalidating an entire patient identification program. *Whalen*, 429 U.S. at 601-02.

72. *Westinghouse*, 638 F.2d at 578 (public interest in research justified intrusion into privacy of employees medical records); Faison v. Parker, 823 F. Supp. 1198, 1201 (E.D. Pa. 1993) (inmate's constitutional right to nondisclosure of medical information outweighed by public interest in access). When deciding whether an intrusion into an individual's privacy is justified certain factors should be considered, such as the type of record, the information contained, the potential for harm from disclosure, the injury from disclosure on the relationship which generated the record, the adequacy of safeguards, and the need for access. *Westinghouse*, 638 F.2d at 578. In determining invasion of privacy it is important to consider whether there is a statute, public policy, or other recognizable public interest. *Id.* "[E]ven material which is subject to protection must be produced or disclosed upon a showing of proper governmental interest." *Id.*

73. Peninsula Counseling Center v. Rahm, 719 P.2d 926, 929 (Wash. 1986) (en banc). The state interest in maintaining adequate mental health facilities and ensuring care for individual patients was a valid governmental interest. *Id.* The court held that disclosure of psychiatric patient names and diagnosis was reasonably necessary to satisfy the valid governmental interest. *Id.* The court refused to allow the individual health centers to encode the information before sending it to the governmental agency, since it "undoubtedly would be more cumbersome and error prone than having one centrally located encoding system." *Id.*

74. The government requires a physician to report treatment for certain wounds, injuries, poisonings, and suspected child abuse. Martin v. Baehler, No. 91C-11-008, 1993 WL 258843, at *3 (Del. Super. Ct. May 20, 1993).

75. *Whalen*, 429 U.S. at 589 (constitutional right to privacy in the doctor-patient relationship). The physician-patient privilege is a patient's right not to have the communications with his or her physician divulged. BLACK'S LAW DICTIONARY 1126 (6th ed. 1990).

lege was designed to protect a patient's confidential information from discovery by a third party.[76] This confidential relationship promotes candid disclosure of information between the patient and the physician, which fosters the best possible medical treatment and diagnosis.[77] The medical profession imposes a duty of physician-patient confidentiality on all physicians[78] by requiring them to take the Hippocratic Oath.[79]

The physician-patient privilege does not create an absolute incapacity[80] of the physician.[81] The scope of the privilege is determined by balancing the patient's interest in protection with the interests advanced by disclosure.[82] When disclosure is necessary, the courts must then ad-

---

This privilege can only be waived by the patient. *Id.* at 1127. Physician-patient privilege was intended to prevent "the humiliation of the patient that might follow disclosure of his ailments." Terre Haute Regional Hospital, Inc. v. Trueblood, 600 N.E.2d 1358, 1361 (Ind. 1992) [hereinafter *Trueblood*].

76. Goodwin v. State, 573 N.E.2d 895, 897 (Ind. Ct. App. 1991). Medical records and financial statements are privileged and require limited disclosure. Jo Ellen Smith Psychiatric Hosp. v. Harrell, 546 So.2d 886, 890 (La. Ct. App. 1989) [hereinafter *Harrell*]. Congress has been hesitant to codify the physician-patient privilege in a federal statute. Mann v. University of Cincinnati, 824 F.Supp. 1190, 1197 (S.D. Ohio 1993). However, the duty to protect a patients confidentiality is recognized by the medical profession, the legislature, and the courts. *Martin*, 1993 WL 258843 at *4. The information obtained through the physician-patient relationship is "extremely private matters warranting a high degree of protection." Tucson Medical Center Inc. v. Rowles, 520 P.2d 518, 524 (Ariz. Ct. App. 1974) [hereinafter *Rowles*]. The protection prevents any disclosure by a physician, unless waived by the patient. *Id.* The legal protection is provided at the time disclosure is attempted, instead of applying a remedy after the violation. *Id.*

77. *Trueblood*, 600 N.E.2d at 1360-61.

78. The breach of physician-patient confidentiality constitutes a tort, entitling the patient to recover damages. *Martin*, 1993 WL 258843 at *4.

79. "Whatever, in connection with my professional practice, or not in connection with it, I see or hear in the life of men, which ought not to be spoken of abroad, I will not divulge as reckoning that all such should be kept secret." *Martin*, 1993 WL 258843 at *3 (quoting Hippocratic Oath). Even the American Medical Association (AMA) cites in its medical ethics "[a] physician shall respect the rights of patients, . . . and shall safeguard patient confidences within the constraints of the law." *Id.* (quoting AMA Principles of Medical Ethics).

80. Incapacity in this instance is referring to a physician's inability to exercise a vested right, such as speech. BLACK'S LAW DICTIONARY 760 (6th ed. 1990).

81. *Goodwin*, 573 N.E.2d at 897. The physician-patient privilege is not an absolute bar to a physician's testimony, but allows the patient the right to exclude the testimony of his physician. State ex rel. Gonzenbach v. Eberwein, 655 S.W.2d 794, 796 (Mo. Ct. App. 1983).

82. Mann v. University of Cincinnati, 824 F.Supp. 1190, 1198 (S.D. Ohio 1993). The physician's duty of confidentiality is outweighed by the justification for disclosure when there is a need to protect the safety of the patient or others. Rea v. Pardo, 522 N.Y.S.2d 393, 396 (N.Y. App. Div. 1987). A student brought a lawsuit against a University for sexual harassment and taking unfavorable academic actions against her. *Mann*, 824 F.Supp. at 1192. The plaintiff filed a motion for a protective order and sanctions due to the unauthorized release of her medical records. *Id.* at 1191-92. The medical records disclosed exceeded the production request and contained private information which was irrelevant to

dress who is privileged to access and disseminate the information.[83] This determination must include the reason behind the disclosure and the extent of the release.[84]

When neither the patient nor physician are in a position to assert the privilege, the hospital has a duty to assert the privilege over the hospital records.[85] Thus, the physician-patient privilege protects the medical record from unwarranted disclosure and should be asserted by anyone who has a duty to protect the patient's confidentiality. However, the privilege does not prohibit all third party access to medical records.

B. THIRD PARTY ACCESS TO MEDICAL INFORMATION

The release of medical information to a third party payer[86] produces doubts regarding the sufficiency of protection for a patient's private medical information. The insurance industry collects, maintains, and utilizes enormous amounts of personal information concerning its clientele.[87] This information is frequently transmitted to the Medical Information Bureau (MIB)[88] for use by other subscribers in the insurance industry.[89] Despite this practice, the physician-patient privilege is not waived when the patient authorizes the release of privileged medical information to third parties.[90]

---

the lawsuit. *Id.* at 1192. The court granted the protective order and held that the medical records were privileged. *Id.* at 1197. The University was prohibited from disclosing any medical information which exceeded the subpoena duces tecum. *Id.* at 1205-06.

83. Gerwin, *supra* note 52, at 118.

84. *Id.*

85. *Rowles*, 520 P.2d at 523. When a physician's notes are incorporated into the hospital record, they are protected by the physician-patient privilege. *Id.* at 521. The scope of the physician-patient privilege does not change simply because care is rendered in a hospital instead of the home. *Id.* at 520. As a custodian, the producer of a medical record has a duty to protect the record from unjustified intrusion. *Mann*, 824 F. Supp. 1199.

86. A third party payer is an organization that pays the health expenses of those they insure. BRUCE, *supra* note 2, at 198.

87. TRUBOW, *supra* note 65, ¶ 8.01. The insurance industry's large volume of information reflects the huge number of customers it serves. *Id.*

88. The MIB is an index of medical information about applicants for use in underwriting life and health insurance. TRUBOW, *supra* note 65, ¶ 8.02[1] at 8-10.

89. The MIB is an association which conducts a confidential exchange of information among approximately 700 life insurance companies. Senogles v. Security Benefit Life Ins. Co., 536 P.2d 1358, 1360 (Kan. 1975). An applicant for health insurance brought an action against an insurance company for invasion of privacy when it communicated medical information to a third party, the MIB. *Id.* at 1359. The Court recognized that the MIB serves an invaluable function in the life insurance industry and held that there was a valid business interest in the communication of medical information justifying a qualified privilege. *Id.* at 1364.

90. *Gonzenbach*, 655 S.W.2d at 796. The plaintiff in a wrongful death action sought to obtain the medical records that defendant had authorized for release to his insurers. *Id.*

Insurance companies have a qualified privilege[91] to collect and disseminate client information, as long as the disclosure is motivated by a legitimate business interest.[92] Once a qualified privilege applies, an insurance company is only liable for communications which abuse the privilege.[93] Thus, insurance companies have a qualified privilege to collect and disseminate patient information, which does not violate the protection of confidentiality provided by the physician-patient privilege. The question that arises is what protection does patient information receive when it is collected and stored in computerized data banks?

V. PROTECTION OF COMPUTERIZED INFORMATION

President Clinton's health care proposal is dependent upon a completely automated information system.[94] The increasing use of computerized technology for the collection and storage of personal information threatens a patient's right to privacy.[95] Computers promote the collection and analysis of medical records and patient information, therefore creating a "dossier" on every person whose information is in the computer system.[96]

---

at 795. The records involved medical treatment received immediately after the accident. *Id.* The court held that the authorized release of information allows medical records to be released to insurance companies and does not waive the physician-patient privilege, because insurers are considered an integral part of the treatment process. *Id.* at 796.

91. A qualified privilege is a defense in a defamation action when the publication was in a reasonable manner and for a proper purpose. BLACK'S LAW DICTIONARY 1241 (6th ed. 1990). The requirements for a qualified privilege are good faith, an interest or duty to be upheld, a statement limited in its scope to that purpose, a proper occasion, and publication in a proper manner and to the proper parties only. Edwards v. Univ. of Chicago Hosp. and Clinics, 484 N.E.2d 1100, 1104 (Ill. App. Ct. 1985).

92. *Edwards*, 484 N.E.2d at 1104. A mother brought a defamation action, on behalf of her 14 year old daughter, against the hospital after it submitted the diagnosis of "atopic pregnancy" to the insurance company. *Id.* at 1102. The court held that the disclosure of the diagnosis was directly related to a legitimate business interest and was protected by a qualified privilege. *Id.* at 1105. *See also* Millsaps v. Bankers Life Co. 342 N.E.2d 329, 335 (Ill. App. Ct. 1976) (transmittal of code number to MIB considered a legitimate business interest and access to information came within privilege doctrine).

93. *Edwards*, 484 N.E.2d at 1105.

94. *American Health Security Act*, *supra* note 1, at S-35.

95. Gerwin, *supra* note 52, at 115. "[V]ast amounts of personal information are contained not only in medical files but in computerized data banks or other massive government files, much of which is personal in character and potentially embarrassing or harmful if disclosed . . . ." Mann v. University of Cincinnati, 824 F.Supp. 1190, 1199 (S.D. Ohio 1993).

96. Peninsula Counseling Center v. Rahm, 719 P.2d 926, 930 (Wash. 1986) (Pearson, J., dissenting) [hereinafter *Rahm*]. Justice Pearson argued that society has resigned itself to the inevitability of invasion into private affairs, due to the widespread use of computers. *Id.* The courts opinion merely reflects societies apathy. *Id.* Justice Pearson emphasized that today's computer data is tomorrow's dossier. *Id.*

The Supreme Court has acknowledged the implicit threat to privacy of computerized data banks, which accumulate vast amounts of personal information.[97] Nonetheless, the Court declined to address appropriate security measures.[98] Consequently, Congress developed the Privacy Act[99] in response to its concerns over the potential abuse of computerized technology and sophisticated information systems.[100] The Privacy Act is aimed at protecting the privacy of individuals identified in federal information systems and preventing misuse of the information.[101]

Even if unauthorized disclosures do not actually occur, many patients may decline to seek necessary medical care out of fear that their personal information is easily accessible in a computerized file.[102] In *Whalen v. Roe*, the Supreme Court acknowledged that some patients may refrain from using certain medical services due to concerns over

97. Whalen v. Roe, 429 U.S. 589, 605-06 (1977). The *Whalen* Court addressed whether a state could record identifiable patient information in a centralized computer file. *Id.* at 591. "The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed." *Id.* at 605.

98. *Id.* at 605-06. The Court relied on the fact that the right to utilize personal information for public purposes is usually accompanied by a statutory or regulatory duty to prevent unauthorized disclosures. *Id.* at 605.

99. 5 U.S.C.A. § 552a (1993). The Privacy Act provides that "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of the individual to whom the records pertains. . . ." *Id.* at § 552a(b). A "system of records" is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." *Id.* at § 552a(a)(5).

100. Thomas v. United States Dep't of Energy, 719 F.2d 342, 345 (10th Cir. 1983). An employee sued the Department of Energy claiming a violation of the Privacy Act after his supervisor disclosed to coemployees that he had been sent for a psychiatric evaluation. *Id.* at 343. The supervisor learned of the plaintiff's condition through oral conversations and not from the system of records. *Id.* at 344. The court held that a cause of action under the Privacy Act can only be sustained when the initial information was acquired directly from the system of records. *Id.* at 345.

101. *Id.* at 345-46. Lawsuits brought for a violation of the Privacy Act are limited to actions against the United States Government. Unt v. Aerospace Corp., 765 F.2d 1440, 1447 (9th Cir. 1985).

102. Whalen v. Roe, 429 U.S. 589, 600 (1977). Patients will be reluctant to seek medical treatment when there is a fear that his or her medical information will become public and affect their reputation or embarrass them. *Mann*, 824 F.Supp. at 1199. A person's self perception and relationship to society can change with the knowledge that every transaction is stored in a computerized database. Graham, *supra* note 8, at 1396.

the availability of personal information.[103] Yet, the Court condoned the disclosure, because the statute did not deprive the public access to treatment.[104]

Justice Brennan's concurring opinion emphasized that the computerized storage of confidential information did not render the state's legitimate collection and storage of data unconstitutional.[105] Thus, computerized information receives the same protection as the more traditional methods of data collection. Still, the accessibility of computerized information breeds doubts concerning the sufficiency of safeguards for the protection of patient information.

A. THE COURT'S PROTECTION OF PATIENT INFORMATION

Computerized information without adequate safeguards poses a threat to the confidentiality of medical information. Patient information can be publicly disclosed when employees fail to maintain proper security, when data is disclosed as evidence in a lawsuit, and when information is voluntarily revealed.[106] Courts have repeatedly declined to memorialize the extent of security measures necessary for the protection of computerized data banks which accumulate and store personal information.[107] Therefore, we can only infer what constitutes adequate security measures for computerized information by analyzing a broad range of cases.

In *Whalen*, the Supreme Court determined that vaults and locked cabinets surrounded by a fence with an alarm were adequate protection for confidential information.[108] Nevertheless, the Court declined to decide any question of unauthorized disclosure of accumulated private data with lesser security measures.[109] While the courts have not mandated the security measures utilized in *Whalen*, they may consider

103. *Whalen*, 429 U.S. at 603.

104. *Id.* The court held that the patient identification requirement did not have a sufficient impact, immediate nor threatened, on a patient's reputation or independence to "constitute an invasion of any right or liberty protected by the Fourteenth Amendment." *Id.* at 603-604.

105. *Whalen*, 429 U.S. at 606-07 (Brennan, J., concurring). The Constitution limits the means a state can use to gather certain types of information, because "[the] central storage and easy accessibility of computerized data vastly increase the potential for abuse. . . ." *Id.* at 607. Justice Brennan emphasized that future developments may demonstrate the need for some type of curb on computer technology. *Id.* In light of the carefully designed program and safeguards in *Whalen*, the computerized storage of information did not threaten an individual's constitutional privacy interest anymore than traditional approaches to reporting. *Id.* at 606-07.

106. *Whalen*, 429 U.S. at 589.

107. *Faison*, 823 F. Supp. at 1204.

108. *Whalen*, 429 U.S. at 605.

109. *Id.* at 605-06.

those security measures whenever addressing the sufficiency of safeguards against disclosure of confidential information.[110]

Courts have found the extraction of individual patient identities from the medical record to be adequate protection of confidentiality.[111] Adequate protection has even been found where a party merely stamped "confidential" in bold letters on a report.[112]

The perimeters for adequate safeguards are very broad. Courts seem reluctant to render any safeguard inadequate, relying on the fact that public disclosure of confidential medical information is expressly prohibited.[113] Therefore, the measure of adequate safeguards for confidential information remains inconsistent. Only the legislature can standardize the management of confidential information.

B. SECURITY MEASURES IN THE HEALTH SECURITY ACT

At the core of President Clinton's proposal for a nationwide health plan is electronic technology.[114] This technology ranges from the automated health security card to a nationwide electronic database capable of managing enormous amounts of patient information.[115] The Act provides safeguards for the protection of privacy in health care information by proposing health information system standards.[116] However, the Act does not mandate the development and implementation of security standards until years after the Act's enactment.[117] Uniform security standards are imperative to protect the privacy of patient information and must be applicable to anyone who has access to patient information.[118] The Act's failure to implement security standards at the time of enactment will have an impact on the lives of everyone who utilizes the health care system.

---

110. *Faison*, 823 F. Supp. at 1204.

111. Terre Haute Regional Hosp., Inc. v. Trueblood, 600 N.E.2d 1358, 1359 (Ind. 1992) (removal of identifying information from medical records for discovery purposes considered adequate protection) [hereinafter *Trueblood*]; *See also* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 580 (3d Cir. 1980) (removal of names and addresses of individuals for research study considered adequate protection) [hereinafter *Westinghouse*]. A patient sought to inspect and copy hospital records of non-party patients. *Trueblood*, 600 N.E.2d at 1359. The court held that redacting all identifying information regarding non-party patients from the record was an adequate safeguard and did not violate the physician-patient privilege. *Id.*

112. *Faison*, 823 F. Supp. at 1204.

113. *Id.* The court declined to find safeguards inadequate, even though the information was maintained in court, probation, prison, and attorney files. *Id.*

114. *American Health Security Act*, *supra* note 1, at S-35.

115. *Id.*

116. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5120(a) (1993).

117. *See supra* note 45.

118. Bob Francis, *The Search for Client/Server Security*, DATAMATION, May 1, 1993, at 39.

A computer's most enchanting feature is the accessibility of vast quantities of information.[119] Anyone with access to a computer could potentially view unlimited amounts of personal information, especially if the computer is part of a network.[120] The need to secure patient information is critical to the protection of patient privacy.[121]

Since no security system is absolutely safe,[122] multiple security measures are necessary to insure the integrity of a patient information network.[123] Physical control, which limits physical access to the computer, is the most basic security tactic.[124] Computers should be kept out of high traffic areas[125] and should not be left unattended.[126] Computer areas surrounded by walls and doors restrict access to the protected entrance.[127] Card readers and keypads can insure that only authorized persons gain access to the computer area.[128] Closed circuit cameras[129]

---

119. Herb Brody, *High Anxiety*, PC-COMPUTING, Nov. 1988, at 214. Modern computer technology provides for the storage of vast amounts of sensitive information such as medical records, which are easily transferable. Renae Angeroth Franks, Note, *The National Security Agency and Its Interference with Private Sector Computer Security*, 72 IOWA L. REV. 1015, 1017 (1987).

120. Brody, *supra* note 127, at 214. The three major types of computer technology used to organize a system are mainframe, minicomputer, and office automation. PHILIP E. FITES ET AL., CONTROL AND SECURITY OF COMPUTER INFORMATION SYSTEMS 131 (1989) Office automation is the linking of personal computers into a network. *Id.* Mainframes and some minicomputers handle large amounts of information and may have hundreds of users. *Id.* at 132-33.

121. Francis, *supra* note 126, at 39. Security and confidentiality are "absolutely imperative" when dealing with patient information. Amy Schurr, *How Two Universities Developed Client/Server Applications*, PC WEEK, Aug. 23, 1993, at 103. A development group from the University of Chicago and the University of Illinois produced a client/server program, which stores a patient's medical information and prescriptions, schedules appointments, and has accounting and billing capabilities. *Id.* The data is entered on the client end and the medical records are stored on the server, which is kept in a vaulted room. *Id.*

122. Robert J. Sciglimpaglia, Jr., Comment, *Computer Hacking: A Global Offense*, 3 PACE Y.B. INT'L L. 199, 241 (1991).

123. Francis, *supra* note 126, at 39-40.

124. DAN M. BOWERS, ACCESS CONTROL AND PERSONAL IDENTIFICATION SYSTEMS 59 (1988). Magnetic tape, diskettes, and other media should be stored in an area which can be restricted, controlled, locked, and protected from fire. FITES, *supra* note 128, at 124-25.

125. COREY SANDLER ET AL., VAX SECURITY PROTECTING THE SYSTEM AND THE DATA 192 (1991). Furniture may need to be rearranged to provide the best security angle. *Id.* at 194.

126. *Id.* at 146. Computer security breaches are most frequently committed by insiders at a terminal which is neglected and unguarded. Deborah L. Wilkerson, Comment, *Electronic Commerce Under the U.C.C. Section 2-201 Statute of Frauds: Are Electronic Messages Enforceable?*, 41 U. KAN. L. REV. 403, 426 (1992). A computer can be protected by a locking mechanism that only allows access when unlocked by a device that reads a credit card sized "key." Francis, *supra* note 126, at 40.

127. BOWERS, *supra* note 132, at 59. Physical security can be a fence, locked door, or video observation. FITES, *supra* note 128, at 117.

128. ACCESS CONTROL AND PERSONAL IDENTIFICATION, *supra* note 132, at 60.

and alarm systems may also deter the unauthorized access to the computer system.[130] However, physical control alone is not enough to adequately secure the privacy of computerized information.

Access control is the most effective security measure to protect the confidentiality of computerized information, because it prohibits access to information even if a person has gained physical access to the computer area.[131] Access controls should be built into every terminal which has access to the network. User identification codes,[132] passwords,[133] encryption,[134] audit trails[135] and callback devices[136] are highly sophisti-

129. SANDLER, *supra* note 133, at 192.

130. BOWERS, *supra* note 132, at 59.

131. *Id.*

132. User identification codes identify the individual seeking access to the network and correspond to the user account. Cheryl S. Massingale & A. Faye Borthick, *Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services*, 12 W. NEW ENG. L. REV. 167, 190 (1990). Storage lockout is a key security measure which restricts users access to certain drives. *See* Francis, *supra* note 126, at 40.

133. Passwords validate a user as the owner of a user identification codes. Massingale & Borthick, *supra* note 140, at 190. Passwords are the easiest and most effective access control. FITES, *supra* note 128, at 214. A system will not allow access without the correct identification and password. *Id.* The United States government suggests computers have multi-level passwords. Sciglimpaglia, *supra* note 130, at 242. A computer can be equipped with a "walk-n-lock" feature, which password protects a computer that is not used after a preset time. Francis, *supra* note 126, at 43. The Government recommends that a computer systems disconnect after a limited number of incorrect passwords. Sciglimpaglia, *supra* note 130, at 242. Alarms and locks can be activated after a preset amount of unsuccessful log-in attempts. Francis, *supra* note 126, at 40. A central sign on feature allows easy yet restricted access to networked information from any personal computer, through the use of one central password. *Id.* Even better than the password are tokens, which contain the password and identification. *Id.*

134. Encryption changes plaintext into ciphertext, through the use of an encryption unit and encryption key. FITES, *supra* note 128, at 196. Encrypting passwords is a sophisticated security measure for protecting access to the network. Massingale & Borthick, *supra* note 140, at 190. Encrypted information cannot be utilized or even read without the encryption algorithm and the key to the code. BOWERS, *supra* note 132, at 59. Information is sent through an encryption algorithm and is decrypted on the receiving end. Wilkerson, *supra* note 134, at 425. Decryption utilizes a key to convert ciphertext back into plaintext. FITES, *supra* note 128, at 196. A high level security measure involves a set of public and private cryptographic keys, which identify the user by key number, name, and location. Wilkerson, *supra* note 134, at 425.

135. Audit trails track a user's session and foster the detection of security breaches. Francis, *supra* note 126, at 40. The Government recommends keeping system logs. Sciglimpaglia, *supra* note 130, at 242. All attempted access should be logged with subsequent investigation of suspicious activity. Massingale & Borthick, *supra* note 140, at 191.

136. Callback devices validate the calling computer terminal and operator. BOWERS, *supra* note 132, at 58. The computer requests the identity of the calling terminal, disconnects and calls the telephone number in the computer's file for the calling terminal. *Id.* at 60.

cated access controls which prevent unauthorized access to computerized information.

Even if a user is authorized to access computerized information, an important security measure is information control, which restricts the type and amount of information a user may access.[137] The operating system determines which files a user may access[138] and should be allowed no more access than is reasonably necessary to meet a users specific purpose.[139] The days and times a user can log into the system can also be restricted through timed lockout.[140]

If the Act is to genuinely protect the privacy of patient information, specific security standards for the protection of computerized information need to be implemented and strictly enforced at the time of the Act's enactment. Otherwise, the fate of everyone's personal information is dependent upon the ethics and responsible handling of anyone with access to the network. This places an even greater burden on an already overwhelmed health care industry. The burden of protecting patient privacy should be on the legislature to standardize the entire health care industry at the time the Act is ratified.

VI. CONCLUSION

As the United States prepares to implement a national health care plan, it is computer technology that makes this vision a reality. With the widespread use of electronic information systems, the need for protection of individual privacy is greater than ever.

The consolidation and analysis of patient information can be of tremendous benefit to the medical community in rendering high-quality patient care.[141] However, the individual patient's interest in privacy is often outweighed by the disclosure needs of physicians, lawyers, insurers, and government. Both the need for disclosure and the interest in privacy must be considered in the development of standards for the handling and storage of computerized medical information.

In light of the Act's prevailing use of computers, every American who utilizes the health care system will be threatened by potential unwarranted disclosure of his or her intimate medical information. At

137. Sciglimpaglia, *supra* note 130, at 242.

138. BOWERS, *supra* note 132, at 59.

139. The Act restricts disclosure of individually identifiable health information to the minimal amount necessary to accomplish the purpose for disclosure. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5120(c) (1993).

140. Francis, *supra* note 126, at 40.

141. Information systems foster the analysis of a patient's physical status and health trends. *American Health Security Act*, *supra* note 1, at S-35. It also encourages the evaluation of the health care system. *Id.* Computerized information systems facilitates the identification of fraudulent activities. *Id.*

this point, the Act does not specify the security measures to be standardized and allows several years for development and implementation.[142] This failure to address the privacy implications of computerized information jeopardizes the individual patient's right to privacy and renders a complete patient "dossier" easily accessible. If privacy is to be truly protected, it is imperative that specific security standards and strict sanctions[143] for unauthorized disclosure of computerized medical information be clearly defined before the Act is ratified. Otherwise, an individual's constitutional right to privacy in his or her medical record will be lost in the Act's relentless ambiguity.

Congress has the sole authority and duty to protect the privacy of Americans. To protect our privacy, it is imperative that Congress standardize security measures for computerized medical information and allow no more disclosure than is reasonably necessary. Only then can Americans have true "health security."

Susan E. Corsey

142. *See supra* note 45.

143. A violation of the health information system standards will result in a civil money penalty of not more than $10,000 for each violation. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5141(a)(3) (1993). This penalty includes the use of the Health Security Card for other than its intended purpose. H.R. 3600/S. 1757, 103d Cong., 1st Sess. § 5141(a)(2) (1993).