Fordham Urban Law Journal

Volume 25 | Number 1 Article 6

1997

Telemedicine Today and Tomorrow: Why "Virtual" Privacy Is Not Enough

Christina M. Rackett

Telemedicine Today and Tomorrow: Why "Virtual" Privacy Is Not Enough

Cover Page Footnote
J.D. Candidate, Fordham University, 1998; B.A., summa cum laude, New York University, 1995. The author thanks John, Trudy, and Kimberly Rackett for their tireless support and encouragement, and Jaie Solis for his infinite patience.

TELEMEDICINE TODAY AND TOMORROW: WHY "VIRTUAL" PRIVACY IS NOT ENOUGH

*Christina M. Rackett**

Introduction

Today's telemedicine technology may conjure up thoughts of science fiction fantasies,[1] but it has existed since the 1950s.[2] Telemedicine, or "remote electronic clinical consultation,"[3] permits patients and doctors in different locations to communicate with each other for diagnostic or educational purposes. Communication is accomplished through the use of everyday means, such as telephones and fax machines,[4] as well as more sophisticated tools, including electronic stethoscopes, high resolution cameras,[5] interactive television or computer lines,[6] and satellites.[7]

Telemedicine benefits patients in underserved,[8] remote areas[9] by increasing access to quality and specialized medical care. For ex-

---

* J.D. Candidate, Fordham University, 1998; B.A., *summa cum laude*, New York University, 1995. The author thanks John, Trudy, and Kimberly Rackett for their tireless support and encouragement, and Jaie Solis for his infinite patience.

1. For example, telemedicine can enable a doctor in one location to direct robotic equipment to perform surgery on a patient in another location. *See* Marilyn Hanzal, *Telemedicine: 'Beam Me Up, Doctor'*, CHI. DAILY L. BULL., May 20, 1996, at 5.

2. *See* Douglas D. Bradham et al., *The Information Superhighway and Telemedicine: Applications, Status, and Issues*, 30 WAKE FOREST L. REV. 145, 149 (1995). The first telemedicine project was an interactive audio system which linked seven hospitals in Nebraska, Iowa, North Dakota, and South Dakota for weekly mental health lectures. *See id.*

3. Telemedicine Research Center, *What Is Telemedicine* (visited Sept. 26, 1996) <http://tie.telemed.org>.

4. *See* Phyllis F. Granade & Jay H. Sanders, *Implementing Telemedicine Nationwide: Analyzing the Legal Issues*, 63 DEF. COUNS. J. 67, 67 (1996).

5. *See id.*

6. *See* Tony Cappasso, *Telemedicine: The Latest Technology Is Bringing Doctors and Far-Away Patients Closer Together*, ST. J.-REG. (Springfield, Ill.), Aug. 4, 1996, at 15.

7. *See* Telemedicine Research Center, *supra* note 3.

8. For a discussion of why there is a shortage of physicians in rural areas, *see generally* Daniel McCarthy, Note, *The Virtual Health Economy: Telemedicine and the Supply of Primary Care Physicians in Rural America*, 21 AM. J.L. & MED. 111 (1995).

9. These locations include primarily rural and inner city areas, which often lack sufficient available medical care; prisons and mental health institutions, where transporting sick patients to outside doctors requires extra staff and brings security risks; and nursing and private homes, where patients may not be able to travel to doctors unaided. *See* Elizabeth Neus, *Telemedicine Hailed as Future Wave of Industry But Detractors Claim Barriers Doom Idea*, HOUS. POST, Mar. 19, 1995, at A5.

ample, a general practitioner in a rural town can link via telemedicine to a cancer specialist at a prestigious urban medical center for immediate advice on how to most effectively treat a patient. The use of telemedicine to share medical expertise and cutting-edge procedures has already saved lives.[10]

Telemedicine also decreases the cost of medical care to isolated patients[11] by reducing patients' and physicians' transportation costs,[12] and by limiting needless tests and duplication of records.[13] In addition, telemedicine's ease in delivering speedy care allows physicians to treat remote patients before symptoms worsen, and before huge medical bills amass.[14]

Telemedicine's benefits,[15] however, are hampered by unresolved patient privacy issues.[16] Because of the easy access, duplication, and linkage capabilities of telemedicine technology, confidential

10. A doctor in an urban hospital recently directed a rural doctor through his first amputation surgery via video, thereby saving the patient's life. *See* Telemedicine Research Center, *supra* note 3. In addition, at least six lives have been saved in Texas due to telemedicine. *See* Sharon McIlrath, *The Bottom Line (Telemedicine, Part 4)*, 38 No. 17 AM. MED. NEWS, May 1, 1995, *available in* 1995 WL 10008741. *See also* Spencer Rich, *Battlefield Medicine Turns Electronic,* WASH. POST, Oct. 18, 1996, at A25 (discussing a United States Army estimate that one-third of American casualties during the Vietnam War could have been saved if there had been an advanced telemedicine program in place).

11. One study estimates that $80 billion spent on American health care could be saved annually by using telemedicine. *See* Jim Barlow, *Telemedicine Faces Struggle*, HOUS. CHRON., Apr. 30, 1995, at 1. In addition, American hospitals currently save 14 to 22 percent per year due to videoconferencing. *See* Marcia H. Pounds, *Future Is Now for Videoconferencing*, SUN-SENTINEL (Ft. Lauderdale, Fla.), Aug. 23, 1996, at 1F.

12. Because telemedicine enables medical services to be rendered without travel, it reduces instances of lost wages and lost time. *See* McIlrath, *supra* note 10; *see also* Telemedicine Research Center, *supra* note 3. Patients need not compensate doctors for "windshield time" spent commuting to a small town to deliver services. *See* McIlrath, *supra* note 10.

13. *See* Neus, *supra* note 9, at A5.

14. *See* Kathleen M. Vyborny, *Legal and Political Issues Facing Telemedicine*, 5 ANNALS HEALTH L. 61, 63 (1996).

15. Other benefits of telemedicine are educational and legal. For example, a doctor in a Texas hospital was prevented from delivering babies because the nurses' neonatal credentials had expired. The nurses then participated in telemedicine video training, received the required credentials, and were able to assist the doctor in 15 deliveries in nine months. *See* McIlrath, *supra* note 10. In addition, telemedicine may lessen medical malpractice liability by enabling doctors to quickly tap important information regarding a patient's condition and medical history, thus resulting in more accurate diagnoses. *See* Rodd Zolkos, *Telemedicine Calls Liability Risks Into Question*, BUS. INS., Oct. 21, 1996, at 3.

16. For an outline of other legal problems surrounding telemedicine, including licensing and medical malpractice issues, *see* Robin E. Margolis, *Law and Policy Barriers Hamper Growth of Telemedicine*, 11 No. 10 HEALTHSPAN 14, 15 (1994).

patient data may be intercepted and misused by non-medical insiders, such as billing clerks and insurers, as well as outside hackers.[17] As a result, particularly vulnerable patients, such as those with AIDS or mental illness, may be denied jobs, credit, insurance,[18] or even their dignity.[19] Telemedicine patients are not adequately protected against such invasions of privacy because states' medical confidentiality requirements are not uniform.[20] As a result, patients are subjected to varying levels of protection depending upon where they live[21] or where their doctor is licensed.

This Note demonstrates the need for federal telemedicine legislation that provides uniform confidentiality protection for all telemedicine patients. Part I details the use of telemedicine and outlines the link between telemedicine and privacy issues. Part II discusses current federal and state privacy law, emphasizing the laws that protect medical information. Part III argues that federal telemedicine legislation is necessary to safeguard the confidentiality of patients' medical records and proposes a uniform law that protects the privacy of telemedicine patients in every state. This Note concludes that without federal legislation, telemedicine will wither, along with isolated patients' hopes of one day receiving quality and affordable medical care.

I. Telemedicine's Rise and Impact on Patient Privacy

Forty years ago, when telemedicine was experimental, doctors conferred with each other by telephone.[22] Today, medical data, comprised of both text and images, can speed across state lines in seconds. Although this improved technology delivers much needed medical care to remote patients in inner cities and rural areas, there are also negative by-products. More people than ever can access patients' personal health information electronically, including those who should not be privy to such information, such as

17. *See infra* notes 53-60 and accompanying text.

18. *See infra* notes 65-68 and accompanying text.

19. *See infra* notes 61 and 73 and accompanying text (describing victims humiliated by the unauthorized disclosure of their personal health information).

20. *See* Lawrence O. Gostin et al., *Privacy and Security of Health Information in the Emerging Health Care System*, 5 HEALTH MATRIX 1, 13 (1995) ("State privacy laws do exist, but they are not uniform . . . .").

21. In California and New York, for example, doctors are prohibited from disclosing the names of HIV-positive patients' sexual partners to the state, while in Colorado and Minnesota, such disclosure is mandatory. *See* Barry B. Cepelewicz, *Telemedicine: A Virtual Reality, But Many Issues Need Resolving*, 13 No. 9 MED. MALPRACTICE L. & STRATEGY 1, 3 (1996).

22. *See* Bradham, *supra* note 2, at 149.

unauthorized "curiosity seekers"[23] and clever hackers.[24] Such unauthorized access can have disastrous personal and professional consequences on victimized patients.[25]

A. The Development of Telemedicine

Telemedicine's beginning in the 1950s was slow, but steady.[26] Doctors progressed from case consultation via audio equipment for educational purposes[27] to communicating with patients via closed-circuit telephone systems[28] and closed-circuit televisions.[29] Major developments in early telemedicine were made by the National Aeronautics and Space Administration (NASA).[30]

---

23. A recent survey of health care professionals by the Healthcare Information and Management Systems Society found that "[f]our of 10 respondents identified internal curiosity seekers' as the No. 1 [security risk], while only 17% identified external breech [sic] of security by computer hackers [as a concern] . . . ." John McCormack, *Conference Survey Confirms Internet, Intranets Are Red Hot*, HEALTH DATA MGMT., Mar. 19, 1997, *available in* 1997 WL 8747811.

24. *See infra* note 60.

25. *See infra* notes 65-68.

26. *See* Leslie G. Berkowitz, *Is There a Doctor in the House?*, 25-JUN COLO. LAW. 19, 19 (1996) ("After a slow evolution using the telephone and fax machines, we are now moving to distance education and remote electronic clinical consultation.").

27. *See* Bradham, *supra* note 2, at 149 (describing weekly teleconferencing lectures linking seven hospitals in four different states).

28. By 1961, psychiatrists were conducting group "telepsychiatry consultation[s]" with distant patients via telephone. *See id.*

29. *See* Cappasso, *supra* note 6, at 15. For example, in 1967, employees and travelers at Logan International Airport received medical treatment from doctors at Massachusetts General Hospital via two-way audiovisual microwave equipment. *See* Telemedicine Research Center, *History of Telemedicine* (visited Sept. 26, 1996) <http://tie.telemed.org>.

30. *See* Telemedicine Research Center, *supra* note 29. Beginning in the 1960s, while missions were in progress, the agency "telemetered" physiological readings from both the spacecraft and the astronauts' space suits. *See id.* NASA later shared its advances in satellite technology in experimental telemedicine programs in remote areas of Arizona and Alaska. *See id.* The 1972-1975 Arizona program, Space Technology Applied to Rural Papago Advanced Health Care [STARPAHC], consisted of a paramedic van supplied with microwave and audio transmission equipment which linked Indian patients on the Papago Reservation to specialists in distant hospitals. And in Alaska in 1971, NASA's first Applied Technology Satellite was used to bring health care to patients in 26 remotes sites via video consultation. *See id.* In addition, NASA has lent its expertise to several disaster relief efforts abroad. The Space Bridge to Armenia program was launched in 1989 to bring United States specialists to earthquake victims in Armenia via telemedicine. The project was later expanded to provide treatment for burn victims after a massive railway accident in Ufa, Russia. *See id.*

Today, telemedicine has gained widespread support and use.[31] The federal government and thirteen states spent a combined $100 million on telemedicine projects in the 1980s.[32] During a single period between 1994 and 1995, federal and state contributions to telemedicine and similar advancements were estimated to reach *more* than $100 million.[33] Sixty percent of all telemedicine projects in this country's hospitals have been developed within the past two years,[34] and twenty-nine percent of rural hospitals were predicted to use telemedicine by the end of 1996.[35]

Recently, the Department of Health and Human Services, in an attempt to increase isolated, underserved patients' access to quality and affordable medical care, announced a decision to spend $42 million in developing 19 telemedicine projects in 13 states.[36] In addition, the National Library of Medicine awarded Washington's Beth Israel Deaconess Medical Center a $2.8 million contract[37] to study issues in telemedicine and other communication technologies. President Clinton signed the Health Centers Consolidation Act in late 1996,[38] which will award $36 million in grants to rural telemedicine developers in 1997 and perhaps more through 2001. Interstate and even international telemedicine projects are flourishing. For example, doctors in Minnesota, Florida, and Arizona are linked via the Mayo Clinic's satellites for consultation purposes.[39] The Caribbean[40] and Bosnia[41] represent two sites[42] of in-

31. One commentator credits improved technology for the boon. *See* McCarthy, *supra* note 8, at 115 ("The resurgence of telemedicine has become possible only because of recent developments in technology . . . . [T]he new systems are smaller, less expensive, and are of increased quality.") (citation omitted).

32. *See* Ray Dussault, *Telemedicine Poses Regulatory Woe*, BUS. J.-SACRAMENTO, Apr. 22, 1996, at 21 (citing a 1995 American Medical Association report). The private sector is spending millions on telemedicine as well. *See id.*

33. *See* Berkowitz, *supra* note 26, at 19.

34. *See Telemedicine Programs Spreading Like Wildfire: But Is It Premature to Embrace the New Technology?*, BACK LETTER, May 1, 1996, at 54.

35. *See id.* (referring to an Office of Rural Health Care Policy study).

36. *See Telemedicine Demonstration Project for Medicare Gets HHS Funding*, MED. UTILIZATION MGMT., Oct. 17, 1996, *available in* 1996 WL 10524253.

37. *See* Lane Cooper, *Telemedicine Market in Embryonic Stage*, WASH. TECH., Oct. 24, 1996, *available in* 1996 WL 11557362. The money will be used to develop "telemedicine computer home stations," in which parents at home can watch their sick infants eat and sleep in the hospital's neonatal intensive care unit. *Id.* In addition, when the infants finally leave the hospital, they can still be observed by the doctors via these monitors. *Id.*

38. 42 U.S.C. § 254c (1997).

39. *See* Ira Breskin, *Telemedicine Gains Ground, But Hurdles To Use Remain*, INVESTOR'S BUS. DAILY, Oct. 10, 1995, at A8.

40. *See* Telemedicine Research Center, *What's New* (visited Sept. 26, 1996) <http://tie.telemed.org>. Massachusetts General Hospital and the Howard University Col-

ternational telemedicine programs that bring quality care to remote patients.

In response to the telemedical boom, groups such as the Center for Telemedicine Law,[43] the Telemedicine Research Center,[44] and the Congressional Ad Hoc Steering Committee on Telemedicine and Health Information[45] were established to further telemedicine's development and to study privacy and other issues[46] arising from the new technology. In addition, numerous web sites devoted to telemedicine issues can be found on the Internet.[47]

Commentators in the healthcare and telecommunications industries expect telemedicine to continue to flourish,[48] making remote consultation "commonplace" in fields that rely on images, such as radiology, pathology, and ultrasound.[49] Video consultation is pre-

---

lege of Medicine are cutting patient travel costs and inconvenience while simultaneously providing specialist care to the Caribbean. *Id.*

41. *See* Cooper, *supra* note 37. A United States Army station in Maryland is using telemedicine to observe the troops' health overseas. *Id.*

42. For a detailed account of current telemedicine programs nationwide, *see* Bradham, *supra* note 2, at 152-59.

43. *Telemedicine News: The Quest for Answers to Difficult Legal Questions*, AUTOMATED MED. PAYMENTS NEWS, Dec. 6, 1995, *available in* 1995 WL 2281351. The Center, founded in 1995 by the Cleveland Clinic Foundation, the Mayo Foundation, the Midwest Rural Telemedicine Consortium, and Texas Children's Hospital, studies legal issues that affect telemedicine. *Id.*

44. *See* Telemedicine Research Center, *About the TRC* (visited Sept. 26, 1996) <http://tie.telemed.org>. The Center is a non-profit organization founded in 1994 to further the development of telemedicine. *Id.*

45. The Committee was formed to tackle telemedicine issues at the federal level. *See Implementation of Telecommunication Reforms a Boon to Health Care Providers*, GOV'T PRESS RELEASES, Jun. 12, 1996, *available in* 1996 WL 8788123.

46. The Center for Telemedicine Law, for example, is focusing on licensing and reimbursement questions. *See* AUTOMATED MED. PAYMENTS NEWS, *supra* note 43.

47. *See, e.g.*, <http://tie.telemed.org> (sponsored by the Telemedicine Research Center), <http://www.arentfox.com/telemedicine.html> (sponsored by the Washington, D.C. law firm of Arent Fox Kintner Plotkin & Kahn), <http://www.fcc.gov/Reports/telemed.txt> (sponsored by the government), and <http://www.telemedmag.com> (providing on-line TELEMEDICINE AND TELEHEALTH NETWORKS magazine).

48. *See, e.g., Telemedicine: Fad or Future?*, LANCET, Jan. 14, 1995, at 73. "Conservative" projections of the sales of telemedicine and similar equipment, amounting to just $77 million in 1995, are estimated to approach $100 billion in five years. *See* Cooper, *supra* note 37. In addition, research and development continues to move forward. For example, the Pentagon is developing "battlefield telemedicine" for the future. *See* Rich, *supra* note 10, at A25. The plan includes helmet-mounted cameras to be worn by medics on the scene, which would transmit images of the injured back to doctors in a distant location. Also in the works are personnel status monitors, to be worn by all soldiers, which would transmit any changes in vital signs, as well as positions on the battlefield, to distant medics and doctors. *Id.*

49. *See* LANCET, *supra* note 48, at 73.

dicted to reach more remote areas in the future, such as Antarctica and space stations.[50]

B. The Link Between Telemedicine and Privacy

Telemedicine's risks to patient confidentiality and security of medical information stem from its reliance on computer technology to store, transmit, and retrieve medical records and images. Modern technology permits downloaded information to be accessed, copied, and even forwarded elsewhere with just a few strokes on a computer keyboard.[51] Currently, an estimated 80 people view a patient's health information during a patient's single rendezvous with the health care system.[52] These individuals may include not only medical personnel, but hospital administrators, insurers, researchers, employers, and law enforcement officers.[53] Even though some of these individuals are authorized to access patients' confidential health information, they may fail to guard it properly.[54] In addition, the physicians' obligations of confidentiality in the Hippocratic Oath[55] and the American Medical Associa-

50. *See id.*

51. *See, e.g.*, Community Health Management Information Systems Resource Center, *Health Information Systems and Privacy* (visited Sept. 26, 1996) <http://chmis.org/> ("In an electronic environment . . . unique risks are present from simultaneous access to information from remote areas of the country, ease of duplication and transfer, and the ability to more easily link various systems of records.").

52. *See id.* These individuals may include not only health care personnel like doctors and nurses, but also hospital administrators and insurance companies.

53. *See Hearings on Medical Records Confidentiality Before the Subcomm. on Gov't Management Information and Technology of the House Comm. on Government Reform and Oversight*, 104th Cong. (June 14, 1996) (statement of Janlori Goldman, Deputy Director of the Center for Democracy and Technology), *available in* 1996 WL 10164954 ("Information demands of insurance companies, managed health care companies, researchers, employers and law enforcement are eroding the doctor-patient confidentiality that is central to health care.") [hereinafter *Hearings*].

54. *See* Robert Landauer, *Histories That Hurt*, PORTLAND OREGONIAN, Dec. 17, 1996, at D09 ("[Doctors' and hospitals'] offices are awash in untrained personnel who don't understand how to screen out information that should not be released.").

55. The part of the oath referring to the physician's duty of confidentiality states: "And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secret." Robert M. Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 N.C. L. REV. 255, 267 (1984) (citing 1 HIPPOCRATES 164-65 (W. Jones trans., 1923), *reprinted in* ETHICS IN MEDICINE 5 (S. Reiser, A. Dyck & W. Curran eds., 1977)).

tion's Code of Medical Ethics do not bind these non-medical personnel.[56]

Telemedicine's broad access capabilities could increase the number of individuals who are privy to patients' electronically transmitted medical records,[57] sparking new fears that the information may be intercepted and misused with even greater ease.[58] Current safeguards do not provide adequate protection.[59] Hackers, both clever outsiders as well as disgruntled insiders, can break into systems and obtain confidential information.[60] Numerous cases of misuse of personal health information have been documented. For example, a New York Congresswoman had her medical records, including information about her depression and a suicide attempt, faxed to the media in the midst of her political campaign.[61] In Colorado, a medical student sold patients' confi-

56. The 1992 Code states: "The physician should not reveal confidential communications or information without the express consent of the patient . . . ." Bernard Friedland, *Time to Re-Examine a Venerable Concept in Light of Contemporary Society and Advances in Medicine*, 15 J. LEGAL MED. 249, 257 (1994) (citing AM. MED. ASS'N, CURRENT OPINIONS OF THE COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS, No. 5.05 (1992)).

57. *See* James Rosenblum, *Medical Liability in Cyberspace*, 8 HEALTH LAW. 10, 10 (1995) ("If physician[s'] offices are linked to local hospitals . . . nurses, billing clerks, data processing clerks, etc.[,] will have easy access to extensive amounts of medical information.").

58. *See* Diane M. Gianelli, *Physician Input on Pressing Ethical Issues*, AM. MED. NEWS, July 22, 1996, at 3; *see also* Ilene K. Gotts & Alan D. Rutenberg, *Navigating the Global Information Superhighway: A Bumpy Road Lies Ahead*, 8 HARV. J.L. & TECH. 275, 332 (1995) (citing National Research Council, *Computers at Risk: Safe Computing in the Information Age* (1991)) ("We are at risk. Increasingly, America depends on computers . . . . The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."); Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295, 310 (1995) ("[T]he 'threats and personal harm' from disclosure of health records 'are real and not numerically trivial.") (citation omitted).

59. Current safeguards, such as passwords and access codes, are flawed in that they are inconvenient and not one hundred percent effective. *See* Hanzal, *supra* note 1, at 5.

60. For example, the Pentagon was the victim of 160,000 security breaches of its computer files in 1995. *See* Diane M. Gianelli, *supra* note 58, at 3; *see also* Terri F. Arnold, Note, *Let Technology Counteract Technology: Protecting the Medical Record in the Computer Age*, 15 HASTINGS COMM. & ENT. L.J. 455, 464 (1993) (describing numerous abuses including the disclosure of a woman's AIDS diagnosis to her fellow employees via information on the hospital computer); Sonya Savkar & Robert J. Waters, *Telemedicine—Implications for Patient Confidentiality and Privacy* (visited Aug. 27, 1996) <http://www.arentfox.com.telemedicine.html> (discussing a 1988 breach of an Arizona hospital's computer system by outsiders, and detailing the crimes of infamous hackers Kevin D. Mitnick and Mark Abene).

61. *See Hearings*, *supra* note 53.

dential medical records to malpractice attorneys.[62] And the personal problems of some employees who enlisted the aid of employee assistance programs were publicized throughout the workplace.[63]

Hackers have a large incentive to misuse patients' confidential health information because it can be a valuable commodity to employers, insurers, and others. The potential brokering of this information is therefore quite likely,[64] and quite dangerous. Unauthorized use of this information can have serious consequences on the patient's personal and professional life.[65] Employers might refuse to hire someone whose medical condition will likely generate expensive medical bills.[66] A psychiatric patient could rationally fear that disclosure of his or her records, "if in the wrong hands, could ruin a job opportunity, harm [his or her] reputation, or prevent [him or her] from changing insurance companies."[67] Other cases include instances where individuals were denied employment, insurance, adoption rights, education, or entry into armed services based on health information that they had or could have a certain disease.[68]

The public is well aware of these dangers. Eighty-five percent of respondents to a 1993 poll believed that health care reform should pay attention to the "absolutely essential" or "very important" goal of protecting medical records' confidentiality, a goal they ranked higher than supplying the uninsured with health insurance.[69] Al-

62. *See id.*

63. *See* Tamar Lewin, *Questions of Privacy Roil Arena of Psychotherapy*, N.Y. TIMES, May 22, 1996, at A1.

64. *See* Savkar & Waters, *supra* note 60. The financial incentives for selling personal information are great. *See* Judith B. Prowda, *Privacy and Security of Data*, 64 FORDHAM L. REV. 738, 741 (1995) (noting that the annual profits of the personal information brokering industry are estimated at $3 billion).

65. *See* Savkar & Waters, *supra* note 60, at n.4 ("[I]mproper disclosure [of health information] can deny an individual access to these basic necessities of life, and can threaten an individual's personal and financial well-being.") (citing U.S. Congress, Office of Tech. Assessment, *Protecting Privacy in Computerized Medical Information* (1993)).

66. *See* Linda Kloss, *Patients Must Protect Selves, Join Debate on Keeping Medical Records*, DAYTON DAILY NEWS, July 12, 1996, at 19A.

67. *See Hearings*, *supra* note 53. Out of fear of such occurrences, some patients ask their doctors to abstain from taking notes. *See id.*

68. *See* Landauer, *supra* note 54, at D09 (referring to incidents cited by Rep. Jim McDermott of Washington).

69. *See* Community Health Management Information Systems Resource Center, *Information Privacy: Autonomy and Informed Consent* (visited Sept. 26, 1996) <http://chmis.org/> (citing a survey done by Louis Harris and Associates and Dr. Alan Westin).

most nine out of ten think computers aid others to illegally acquire personal information about them.[70] As a result, more than two-thirds want limitations on the use of all computerized information, health-related or otherwise.[71] Some individuals, fearful of the lack of health care confidentiality, would avoid seeking treatment altogether.[72]

II. Current Privacy Law

The United States Constitution does not provide for an explicit right of privacy. Rather, the Supreme Court has upheld the right to privacy against governmental invasions under the First,[73] Fourth,[74] Fifth,[75] and Ninth Amendments,[76] the Due Process Clause of the Fourteenth Amendment,[77] and the penumbra of freedoms in the Bill of Rights.[78] Some states provide for an explicit right to privacy in their constitutions.[79] Others, following the federal government's lead, do not.[80] The result is a patchwork of federal and state laws governing the somewhat amorphous right to privacy.

---

70. *See id.* In fact, according to a 1992 survey, twenty-five percent of the public believe that their personal medical information had already been wrongfully disclosed. *See Hearings*, *supra* note 53.

71. *See id.*

72. *See* Community Health Management Information Systems Resource Center, *Primer on Privacy* (visited Sept. 26, 1996) <http://chmis.org/> (citing a 1993 survey of adolescents performed by the University of Massachusetts Medical Center); *see also* Adriana Jenkins, *Mental Health Providers Form Market Network*, BOSTON BUS. J., May 24, 1996, at 1 (describing how many therapy patients feel "uncomfortable knowing that their therapist may give personal details of their sessions to an HMO," a procedure commonly practiced in order to determine if patients qualify for additional therapy sessions). This fear of exposing personal information extends to other areas as well. *See also* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress Or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 206 (1992) (citing a 1990 report indicating that a "significant percentage" of those surveyed avoided applying for jobs, credit, or insurance for fear of revealing personal information).

In medicine, the potential public health consequences of this fear could be tremendous. For example, a future disease carrying the same social stigma as AIDS could be disastrous if victims, fearing exposure, were unwilling to seek treatment.

73. *See* Stanley v. Georgia, 394 U.S. 557, 564 (1969).

74. *See* Katz v. United States, 389 U.S. 347, 350 (1967).

75. *See* Boyd v. United States, 116 U.S. 616, 630 (1886).

76. *See* Griswold v. Connecticut, 381 U.S. 479, 486 (1965) (Goldberg, J., concurring).

77. *See* Meyer v. Nebraska, 262 U.S. 390, 399 (1923).

78. *See Griswold*, 381 U.S. at 484-85.

79. *See infra* note 121 and accompanying text.

80. *See, e.g.*, Arkansas' state constitution.

Although the courts and Congress have made numerous efforts to protect patients' confidential medical records in case law[81] and legislation,[82] health information is not given explicit federal privacy protection.[83]

A. General Federal Privacy Law

Justice Brandeis defined the right to privacy both as "the right to be let alone" and "the right most valued by civilized men."[84] Beginning in 1965, the Supreme Court has recognized an implied right to privacy in the Constitution[85] and has attempted to define the parameters of that right.[86] The right to privacy encompasses at least two similar freedoms: the freedom to avoid disclosure of private matters, or the right to confidentiality, and the freedom to make important personal decisions, or the right to autonomy.[87]

Both federal courts[88] and Congress[89] have protected the right to confidentiality. The Federal Privacy Act of 1974 requires that federal agencies, including federally-funded hospitals, adhere to specific privacy standards in the collection, use, and disclosure of

81. *See infra* notes 98-101 and accompanying text.

82. *See infra* notes 103-05 and accompanying text.

83. *See Hearings*, *supra* note 53 ("Presently, there is no comprehensive federal law that protects peoples' health records."). And the battle rages on. *See* Rory J. O'Connor, *Online Privacy Is Hottest Issue on Capitol Hill: Lawmakers Offer Varied Measures*, ARIZ. REPUBLIC, Feb. 9, 1997, at A10 ("Privacy, or more specifically the lack of it in an online world, is the new hot topic on Capitol Hill.").

84. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

85. *See generally Griswold*, 381 U.S. at 485 (1965) (striking down a statute prohibiting use of contraception, discussing a "zone of privacy").

86. *See, e.g.*, Meyer v. Nebraska, 262 U.S. 390, 399-400 (1923) (upholding a right to choose one's own profession); Pierce v. Society of Sisters, 268 U.S. 510, 534-35 (1925) (upholding a right to choose how to educate one's children); Loving v. Virginia, 388 U.S. 1, 12 (1967) (upholding a right to choose whom to marry); Roe v. Wade, 410 U.S. 113, 152-56 (1973) (upholding a woman's right to determine whether to terminate her pregnancy).

87. *See* Barry v. City of New York, 712 F.2d 1554, 1558-59 (2d Cir. 1983) (upholding the city's financial disclosure law for public interest reasons).

88. *See id.* at 1559 ("Most courts . . . appear to agree that privacy of personal matters is a protected interest . . . .") (citations omitted). Cases which have dealt with the confidentiality aspect of the right to privacy include *Whalen v. Roe*, 429 U.S. 589 (1977) (upholding a New York prescription reporting law), *Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 457 (1977) (upholding an act which provided for separation of former President Nixon's personal documents from official ones), and *Eisenbud v. Suffolk County*, 841 F.2d 42 (2d Cir. 1988) (upholding a county's financial disclosure law, despite its privacy implications, because of the public's interest in avoiding conflicts of interest of government employees).

89. *See, e.g.*, Federal Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (1988)).

personal information.[90] For example, agencies are prohibited from disclosing an individual's record without the prior consent of that individual.[91]

Courts have also protected the right to autonomy, focusing on respecting personal decisions made in marriage,[92] procreation,[93] contraception,[94] family relationships,[95] and child rearing and education.[96] The autonomy right guards against governmental intrusion into personal matters affecting the person, such as the right to refuse medical care.[97]

B. Federal Health Care Privacy Law

Federal courts, including the Supreme Court,[98] have noted the right of individuals to keep their health information private.[99] The Court of Appeals in *United States v. Westinghouse* set forth seven widely-used factors to determine if a disclosure of personal infor-

90. *See id.* The act does not apply to private actors, and is therefore typical of federal privacy law. *See infra* note 105 and accompanying text.

91. 5 U.S.C. § 552a(b). There are many exceptions to this rule. *See, e.g.*, § 552a(b)(1) (permitting disclosure to agency employees who have a need for the information to do their job); § 552a(b)(3) (allowing disclosure in the course of "routine use"); § 552a(b)(4) (permitting disclosure to the Bureau of Census for survey purposes); § 552a(b)(5) (allowing disclosure to an individual who requests the information for statistical purposes); § 552a(b)(6) (permitting disclosure to government agencies for historical preservation purposes); § 552a(b)(8) (allowing disclosure if there has been "a showing of compelling circumstances affecting the health of safety of [another]"); § 552a(b)(9) (permitting disclosure to the legislature and its committees); § 552a(b)(12) (allowing disclosure to consumer agencies).

92. *See, e.g.*, Loving v. Virginia, 388 U.S. 1, 12 (1967).

93. *See, e.g.*, Skinner v. Oklahoma, 316 U.S. 535, 541 (1942).

94. *See, e.g.*, Eisenstadt v. Baird, 405 U.S. 438, 454-55 (1972).

95. *See, e.g.*, Prince v. Massachusetts, 321 U.S. 158, 170-71 (1944).

96. *See, e.g.*, Pierce v. Society of Sisters, 268 U.S. 510, 534-35 (1925); Meyer v. Nebraska, 262 U.S. 390, 403 (1923).

97. *See* Cruzan v. Missouri Dep't of Health, 497 U.S. 261, 278 (1990) ("The principle that a competent person has a constitutionally protected liberty interest in refusing unwanted medical treatment may be inferred from our prior decisions.").

98. *See Whalen*, 429 U.S. at 598-600.

99. *See United States v. Westinghouse*, 638 F.2d 570 (3d Cir. 1980) (allowing employees' medical records to be disclosed to the National Institute for Occupational Safety and Health after prior notice is given to the individuals).

> "[A]n employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection. Information about one's body and state of health is matter which the individual is ordinarily entitled to retain within the 'private enclave where he may lead a private life.'"

Id. at 577 (citation omitted). *See also* Doe v. City of New York, 15 F.3d 264, 267 (2d Cir. 1994) (holding that an HIV positive individual whose medical status was disclosed in a press release has a right to privacy in his condition).

mation is an invasion of privacy.[100] The *Westinghouse* test weighs the public interest in disclosure against an individual's right to privacy.[101] Courts have not hesitated to hold against the individual where public health concerns were at issue.[102]

Congress has also attempted to protect the privacy of patients' health information. Current federal privacy statutes include drug and alcohol treatment laws[103] and rules mandating the confidentiality of Medicare recipients' hospital records.[104] The laws apply to government agencies and government-funded entities.[105]

An individual's medical records, however, receive less federal protection than his or her video rental records.[106] As a result, numerous federal laws have been proposed to increase safeguards for confidentiality of medical records. The Medical Records Confidentiality Act of 1995[107] intended to "[e]nsure personal privacy

100. *Westinghouse*, 638 F.2d at 578. Those factors question

> "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."

Id.

101. *See id.* at 578 ("[A]s in most other areas of the law, we must engage in the delicate task of weighing competing interests.").

102. *See* Doe v. Southeastern Pa. Trans. Authority, 72 F.3d 1133, 1143 (3rd Cir. 1995) (applying the *Westinghouse* factors to find in favor of an employer over its HIV-positive employee's privacy right in his medical records).

103. *See* The Drug Abuse Office and Treatment Act of 1972, 42 U.S.C. § 290dd-2 (Supp. V 1993). The Act limits disclosure of patient information to three situations: to medical personnel during emergencies (§ 290dd-2(b)(A)), to researchers and auditors (§ 290dd-2(b)(B)), and to those authorized by a court for good cause (§ 290dd-2(b)(C)). Violators of the Act are punishable by fines. *See id.* § 290dd-2(f). The law provides strict confidentiality bars on the release of patient information by treatment programs.

104. *See* 42 C.F.R. § 482.1 (1982). Hospitals can release the records if required by federal or state law, a court order, or a subpoena. *See id.* § 482.24(b)(3).

105. The laws do not apply to private actors. *See* 42 U.S.C. § 290dd-2(a); 42 C.F.R. § 482.1.

106. *See* Schwartz, *supra* note 58, at 311. *See* The Video Privacy Protection Act, 18 U.S.C. §§ 2710 (1988 & Supp. V 1993). The Act prohibits disclosure of personally identifiable information from the sale or rental of videocassettes. The bill protects individuals' privacy in detail, mandating the destruction of old video records within one year (§ 2710(c)(4)(e)) and providing for the preemption of state laws (§ 2710(c)(4)(f)).

107. S. 1360, 104th Cong. (1995). The Act was referred to the Committee on Labor and Human Resources on October 24, 1995, and hearings were held November 14, 1995. *See United States Bill Tracking, available in* WESTLAW, 1995 U.S. S.B. 1360 (SN).

with respect to medical records and healthcare-related information," and the McDermott Bill[108] intended to protect "privacy of health information in the age of genetic and other new technologies." The Medical Records Confidentiality Act would mandate that doctors obtain a patient's written, detailed consent before disclosing the patient's records, whether for treatment or payment purposes or not.[109] The act provides for civil penalties of up to $250,000 and criminal penalties of up to $500,000 and ten years in prison for improper disclosures.[110] The McDermott Bill prohibits use and disclosure of health information unless the patient grants consent for that specific use.[111] It provides for penalties similar to those of the Medical Records Confidentiality Act.[112] The 104th Congress adjourned before passing either bill.

Legislators and medical professionals have also introduced measures to regulate the confidentiality of medical records. In 1985, the National Conference of Commissioners on Uniform State Laws proposed the Uniform Health-Care Information Act,[113] which defines medical data as sensitive information and details disclosure procedures, such as a prohibition against any release of information without the patient's written authorization.[114] This Act has been adopted in two states.[115] In addition, the Federation of State Medical Boards of the United States recently suggested that states adopt "A Model Act to Regulate the Practice of Medicine Across State Lines,"[116] requiring that the privacy laws of the state in which the model act is passed apply in telemedicine procedures, regardless of the location of patient records.[117]

---

108. H.R. 3482, 104th Cong. (1996). The Bill was introduced on May 16, 1996, and referred to the House Committees on Commerce and Government Reform and Oversight on the same day. *See United States Bill Tracking, available in* WESTLAW, 1995 U.S. H.B. 3482 (SN).

109. *See supra* note 107 §§ 202-03. Currently, patient records may be disclosed for other purposes, such as research, without the individual's consent. *See supra* note 91.

110. *See id.* §§ 301, 302, 311.

111. *See supra* note 108 § 201.

112. *See id.* §§ 301 and 311.

113. Unif. Health-Care Information Act § 1-101—2-105 (1996). The act recognizes that "[t]he movement of . . . health-care information across state lines, access to and exchange of health-care information from automated data banks, and the emergence of multi-state health-care providers creates a compelling need for uniform laws, rules, and procedures governing the use and disclosure of health-care information." *Id.* § 1-101(5).

114. *Id.* § 2-101(a).

115. The two states are Montana and Washington. *See* MONT. CODE ANN. § 50-16-501 (1993); WASH. REV. CODE ANN. § 70.02.005 (West 1992).

116. *See* Telemedicine Research Center, *supra* note 3.

117. *See id.*

C. State Laws Regarding Protection of Medical Information

Because the United States Constitution prevents only governmental invasions of privacy, Congress allows states to create their own laws to protect their citizens from private actors.[118] California, Florida, and Colorado are among a handful of states that enacted such laws.[119] The lack of uniform regulation results in medical privacy laws which vary greatly from state to state.[120]

At least ten states guarantee their citizens an express, albeit general, privacy right.[121] Eight states have developed comprehensive medical confidentiality laws.[122] Some states have medical confidentiality laws which have little practical effect because they are

118. *See* Leslie Sandberg, *Legal and Policy Issues Challenge Telemedicine*, HEALTH MGMT. TECH., Dec. 1. 1995, at 30, *available in* 1995 WL 10024718.

119. *See, e.g.*, Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633, 644 (1994) (holding that the California Constitution's privacy clause "creates a right of action against private as well as government entities"); Heda v. Superior Court, 275 Cal. Rptr. 136 (Cal. Dist. Ct. App. 1990); Soroka v. Dayton Hudson Corp., 1 Cal. Rptr. 2d 77 (Cal. Ct. App. 1991); Rasmussen v. South Fla. Blood Serv., 500 So.2d 533, 536-37 (Fla. 1987). A Colorado statute provides criminal penalties for those who knowingly and impermissibly appropriate another's health information for personal use. *See* Mark L. Gordon & Diana J.P. McKenzie, *The Lawyer's Roadmap of the Information Superhighway*, 13 J. MARSHALL J. COMPUTER & INFO. L. 177, 191 (1995).

120. For example, the majority of

> "states do not have a comprehensive statute that protects the confidentiality of all health information. The legal standard governing the collection and use of health information may depend on the type of information collected . . . the individual or institution collecting it . . . and whether the information is required by a third party for purposes of payment."

Community Health Management Information Systems Resource Center, *Health Information Systems and Privacy* (visited Sept. 26, 1996) <http://chmis.org/>.

121. These states are: Alaska (ALASKA CONST. art. I, § 22), Arizona (ARIZ. CONST. art. II, § 8), California (CAL. CONST. art. I, § 1), Florida (FLA. CONST. art. I, §§ 12, 23), Hawaii (HAW. CONST. art. I, §§ 6-7), Illinois (ILL. CONST. art. I, §§ 6, 12), Louisiana (LA. CONST. art. I, § 5), Montana (MONT. CONST. art. II, § 10), South Carolina (S.C. CONST. art. I, § 10), and Washington (WASH. CONST. art. I, § 7). *See* Frank C. Morris, Jr., *E-Mail Communication: The Next Employment Law Nightmare*, 20 A.L.I.-A.B.A. COURSE MATERIALS J. 49, 51 (1995). Some of these states allow for civil penalties for those who disclose confidential information. *See, e.g.*, 740 ILL. COMP. STAT. 110/15 (West 1997).

122. These states include Rhode Island, Massachusetts, and Wisconsin. Landauer, *supra* note 54, at D09. *See, e.g.*, MASS. GEN. LAWS ch. 175I, §§ 1-22 (1996); R.I. GEN. LAWS §§ 5-37.3-1—3-11 (1956); WIS. STAT. § 146.82 (1995). The comprehensive Rhode Island medical confidentiality laws apply to private actors, including physicians, and clearly require patient consent before health information can be disclosed. *See* R.I. GEN. LAWS § 5-37.3-1—3-6 (1996). There are, however, exceptions to the necessity of obtaining patient consent. *See* R.I. GEN. LAWS § 5-37.3-4 (1996). California and Montana have passed comparable laws. *See* CAL. CIV. CODE §§ 56.10 & 56.11 (West 1997); MONT. CODE ANN. §§ 50-16-525 & 50-16-526 (1996). California's comprehensive set of health care privacy protection laws even treats eavesdroppers on doctor-patient discussions as felons. *See* Marianne Lavelle, *Health Plan Debate Turn-*

not mandatory.[123] Other states protect only citizens having certain health conditions carrying a particular social stigma, such as alcoholism or HIV.[124]

All fifty states require that physicians report specific communicable diseases and sexually transmitted diseases to the state government.[125] Many of those states require that such reports remain confidential[126] and inaccessible to the public.[127] Forty-nine states, however, permit disclosure of this information in certain situations, including cases where individuals are exposed to infectious or sexually transmitted diseases.[128] Some states are more specific than

---

ing to Privacy, NAT'L L.J., May 30, 1994, at A1; *see also* CAL. PENAL CODE § 636 (West 1997).

123. *See, e.g.*, OR. REV. STAT. § 192.525 (1996), encouraging doctors and hospitals to "adopt voluntary guidelines" to protect patients' records from unnecessary disclosure. *See also* MINN. STAT. ANN. § 144.651(16) (1997). The statute simply provides for general patient confidentiality guidelines for hospitals and nursing homes ("Patients and residents shall be assured confidential treatment of their personal and medical records . . . .").

124. These states are: Alabama, Hawaii, Iowa, Kentucky, Maine, Maryland, Massachusetts, Mississippi, New Mexico, Ohio, Pennsylvania, Texas, and Utah. Marianne Lavelle, *State Laws a Patchwork Quilt*, NAT'L L.J., May 30, 1994, at A17. *See, e.g.*, ALA. CODE § 22-11A-54 (1975); HAW. REV. STAT. § 325-101 (1996); IOWA CODE §§ 125.37 & 141.23 (1996); KY. REV. STAT. ANN. §§ 222.271 & 214.625 (Michie 1996); ME. REV. STAT. ANN. tit. 5, §§ 20047 & 19203-D (West 1996); MD. CODE ANN., HEALTH-GEN. I § 8-601 (1996); MASS. GEN. LAWS ch. 111B, § 11 (1996); MISS. CODE ANN. §§ 41-30-33 & 41-34-7 (1996); N.M. STAT. ANN. § 43-2-11 (Michie 1996); OHIO REV. CODE ANN. §§ 3793.13 & 3701.243 (Banks-Baldwin 1997); PA. STAT. ANN. tit. 71, § 1690.108 & tit. 35, § 7607 (West 1996); TEX. HEALTH & SAFETY CODE ANN. § 85.115 (West 1995); UTAH CODE ANN. § 62A-12-284 (1953). California and New York provide the greatest privacy protection for HIV-infected citizens. Lavelle, *supra*, at A17 (citing U.S. Representative Gary Condit of California). *See, e.g.*, CAL. HEALTH & SAFETY CODE § 120980 (West 1997) (punishing individuals who willfully or negligently disclose HIV test results, causing the patient to experience "economic, bodily, or psychological harm").

125. *See* Lawrence O. Gostin et al., *The Public Health Information Infrastructure: A National Review of the Law on Health Information Privacy*, 275 J. AM. MED. ASS'N 1921, 1923 (1996).

126. These states include Florida, Massachusetts, Pennsylvania, Tennessee, and Vermont. *See id.* at 1923. *See, e.g.*, FLA. STAT. ANN. § 384.25 (West 1997); MASS. GEN. LAWS ANN. ch. 111D, § 6 (West 1997); PA. STAT. ANN. tit. 35, § 521.15 (West 1997); TENN. CODE ANN. § 68-10-113 (1996); VT. STAT. ANN. tit. 18, § 1099 (1996).

127. The laws of Alaska, California, Massachusetts, Mississippi, New York, and North Carolina make such provisions. *See* Gostin, *supra* note 125, at 1923. *See, e.g.*, ALASKA STAT. § 09.25.120 (Michie 1996); CAL. GOV'T CODE § 6254 (West 1997); MASS. GEN. LAWS ANN. ch. 66, § 10 (West 1997); MISS. CODE ANN. § 41-91-11 (1996); N.Y. PUB. OFF. LAW § 89 (McKinney 1997); N.C. GEN. STAT. § 130A-374 (1996).

128. *See* Gostin, *supra* note 125, at 1923. States which permit the notification of the infected person's spouse or sexual partner include Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Mississippi, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Pennsylvania, South

others about situations when disclosure is permissible.[129] Only a handful of states provide both criminal and civil penalties for unauthorized disclosure of health information.[130]

California is the only state to develop legislation specifically addressing privacy concerns in telemedicine.[131] The Telemedicine Development Act of 1996[132] requires that a patient give his written and verbal consent before receiving telemedicine treatment and before his identifiable images and/or data are disclosed to others, including researchers.[133]

III. A Whole New Set of Rules

Current federal law is ineffective in dealing with the new privacy problems raised by telemedicine. State laws are not uniform and

---

Carolina, Tennessee, Texas, Utah, Washington, West Virginia, and Wyoming. *See id.* at 1924-25. *See, e.g.*, ALA. CODE § 22-11A-38 (1996); ARIZ. REV. STAT. ANN. § 32-1457 (West 1997); ARK. CODE ANN. § 20-27-302 (Michie 1995); CAL. HEALTH & SAFETY CODE § 121015 (West 1997); COLO. REV. STAT. ANN. § 25-4-1405.5 (West 1997); CONN. GEN. STAT. ANN. § 19a-584 (West 1997); FLA. STAT. ANN. § 455.2416 (West 1997); HAW. REV. STAT. § 325-101 (1996); IDAHO CODE § 39-610 (1997); IND. CODE ANN. § 16-41-7-3 (West 1997); IOWA CODE ANN. § 141.6 (West 1997); KAN. STAT. ANN. § 65-6004 (1996); KY. REV. STAT. ANN. § 311.282 (Michie 1996); LA. REV. STAT. ANN. § 40:1300.14 (West 1997); MINN. STAT. ANN. § 214.25 (West 1997); MISS. CODE ANN. § 41-23-1 (1996); NEB. REV. STAT. § 71-501.02 (1996); NEV. REV. STAT. ANN. § 441A.220 (Michie 1995); N.H. REV. STAT. ANN. § 141-C:18 (1995); N.J. STAT. ANN. § 26:4-41 (West 1997); N.Y. PUB. HEALTH LAW § 2782 (McKinney 1997); N.C. GEN. STAT. § 130A-144 (1996); N.D. CENT. CODE § 23-07.5-02 (1997); OKLA. STAT. ANN. tit. 63, § 1-528 (West 1997); PA. STAT. ANN. tit. 35, § 7609 (West 1997); S.C. CODE ANN. § 44-29-146 (Law. Co-op. 1996); TENN. CODE ANN. § 68-10-115 (1996); TEX. HEALTH & SAFETY CODE ANN. § 81.103 (West 1997); UTAH CODE ANN. § 26-6-3.5 (1997); WASH. REV. CODE ANN. § 70.24.105 (West 1997); W. VA. CODE § 16-3C-3 (1997); WYO. STAT. ANN. § 35-4-133 (Michie 1997).

129. California and New York are among the states which meticulously list all possible justifications for disclosure, while Nebraska and Oregon provide only general disclosure laws. *See* Gostin, *supra* note 125, at 1924. *Compare* CAL. CIV. CODE § 56.10 (West 1997) and N.Y. PUB. HEALTH LAW § 18 (McKinney 1997) *with* NEB. REV. STAT. § 81-668 (1996) and OR. REV. STAT. § 192.525 (1996).

130. *See* Gostin, *supra* note 125, at 1924-25. This small number of states includes California, Michigan, Minnesota, and Oklahoma. *See id. See, e.g.*, CAL. HEALTH & SAFETY CODE § 120980 (West 1997); MICH. COMP. LAWS ANN. § 333.2638 (West 1997); MINN. STAT. ANN. § 144.769 (West 1997); OKLA. STAT. ANN. tit. 63, § 1-502.2 (West 1997).

131. *See* Pamela J. Podger, *Legislators Push for Surgery on Telemedicine*, THE FRESNO BEE, May 18, 1996, at B1. The bill, 1995 CA S.B. 1665, was signed into law by the governor on September 24, 1996, and is known as the Telemedicine Development Act of 1996. CAL. BUS. & PROF. CODE § 2290.5(c)(5) (West 1996).

132. *Id.*

133. Failure to obtain patient consent is considered "unprofessional conduct" by the practitioner. *See id.* Those found guilty of such conduct are subject to disciplinary action by the Division of Medical Quality. *See id.* § 2234.

may provide limited or no protection at all for medical information, let alone electronic health data transmitted via telemedicine. Although the proposed federal laws[134] and California's Telemedicine Development Act of 1996[135] are good first steps, telemedicine requires a whole new set of rules. The prevalence of computer technology in telemedicine makes it easier than ever to access, duplicate, and even transmit private patient images and data for improper purposes. As a result, the best solution for safeguarding patient medical information is federal medical confidentiality legislation that addresses the specific privacy issues raised by telemedicine.

A. Privacy Problems Unique to Telemedicine

Telemedicine's reliance on computer technology to send and receive confidential patient health information raises unique privacy concerns that existing laws cannot solve.[136] As a result of transmitting personal patient health data electronically, telemedicine increases the number of individuals who have, or can obtain, access. Patient information is threatened not only by unauthorized insiders, but also by outside hackers. Those with access can easily copy or forward patient information. The results can be disastrous, not only for the patient himself, who may experience personal and financial harm,[137] but also for future patients, who may refrain from reaping the benefits[138] of this new technology for fear of losing their privacy.[139] As telemedicine continues to grow,[140] this problem is not likely to solve itself.

B. Federal Protection Is Inadequate

Telemedicine patients receive limited protection from the federal government. Because federal laws such as the Federal Privacy Act of 1974[141] generally apply only to government disclosures of private medical information,[142] it is possible that they may protect only five percent of all medical data.[143] The majority of medical

134. *See supra* notes 107-12 and accompanying text.
135. *See supra* note 132 and accompanying text.
136. *See infra* notes 141-53 and accompanying text.
137. *See supra* notes 65-68 and accompanying text.
138. *See supra* notes 8-14 and accompanying text.
139. *See supra* note 72 and accompanying text.
140. *See supra* notes 48-50 and accompanying text.
141. *Supra* note 89 and accompanying text.
142. *See supra* note 105 and accompanying text.
143. *See* Schwartz, *supra* note 58, at 315 (referring to a 1980s estimate).

data, viewed by private actors such as hospitals, insurance companies, and health care providers,[144] are left unprotected.

Current federal laws on medical information and privacy also contain many loopholes, including permitted disclosure for "routine use"[145] by a government agency. In some instances, it is unclear whether federal guidelines are even followed or enforced.[146] The Federal Privacy Act, for example, does not provide for an enforcement agency.[147]

The Supreme Court has expressed concern about the inability of current confidentiality laws to provide sufficient protection from technology's advances.[148] Congress' advisory agency, the Office of Technology Assessment, agreed in its 1986 report, which revealed that "use of new electronic technologies in processing, comparing, and linking personal information has eroded the protections of the Privacy Act."[149] Furthermore, the provision of specific drug and alcohol laws[150] indicates an understanding by Congress that "the [confidentiality] rules for ordinary medical records are either not well defined or are too weak,"[151] and that patients need special safeguards to prevent adverse reactions from employers, insurers, and others in the face of unauthorized disclosures.

C. State Privacy Laws Conflict

State laws are also incapable of handling the privacy concerns arising from the widespread use of telemedicine. The very nature

144. *See id.* at 315.

145. *See id.* at 318 (There are at least 38 "routine uses" that fit into the Federal Privacy Act's "routine use" exception.) (citation omitted); *see also supra* note 99. The existence of loopholes to privacy laws may be particularly dangerous in HIV-positive patient cases. Disclosure of those patients' status can be justified as necessary for individual and public health. *See* Roger Doughty, Comment, *The Confidentiality of HIV-Related Information: Responding to the Resurgence of Aggressive Public Health Interventions in the AIDS Epidemic*, 82 CAL. L. REV. 111, 145 (1994).

146. *See, e.g.*, Gellman, *supra* note 55, at 276 (referring to unlikelihood that Medicare Act's confidentiality mandates are strictly adhered to) (citation omitted).

147. *See* Kathleen A. Linert, Note, *Database Marketing and Personal Privacy in the Information Age*, 18 SUFFOLK TRANSNAT'L L.J. 687, 698 (1995) (citing JAMES MICHAEL, PRIVACY AND HUMAN RIGHTS 83 (1994)).

148. In his concurrence in *Whalen* twenty years ago, Justice Brennan stated that restraints on the advancement of computer technology might be needed in the future to prevent misuse of information about individuals. 429 U.S. at 607 ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.").

149. *See* Prowda, *supra* note 64, at 746 (citation omitted).

150. *See supra* note 107 and accompanying text.

151. *See* Gellman, *supra* note 55, at 277.

of telemedicine requires that patients' confidential medical information move across state boundaries. As a result, it is unclear whether the privacy laws from the patient's state of residence or those from the diagnosing doctor's state apply. This distinction is important because states have taken different approaches to protect the medical data of their citizens.[152] For example, a California patient and an Arkansas patient treated by the same New York specialist via telemedicine may each receive two different standards of privacy protection.[153] A uniform confidentiality standard would eliminate any conflict of laws problems by creating predictability and certainty, thereby encouraging the increased use of telemedicine by patients and doctors.

D. Proposed Laws Are Flawed

Many proposed federal laws have stalled and died in Congress.[154] Although these proposals represent attempts to grapple with the increasing privacy concerns related to telemedicine, many fall short of adequately protecting patients' medical confidentiality.

The Medical Records Confidentiality Act of 1995[155] is flawed because too many groups, including public health agencies, researchers, and large companies, would continue to have authorized access to patient medical information,[156] leaving unsolved the problems of insider access and broad loophole exceptions.[157] In addition, because the bill does not preempt federal drug and alcohol treatment laws and state mental health laws,[158] it does not create a uniform

152. *See supra* notes 118-33 and accompanying text; *see also* Reidenberg, *supra* note 72, at 229 ("Like the federal industry-specific laws, each state law generally seeks to resolve a narrow problem within a given industry and does not systematically address all the privacy concerns relating to the acquisition, storage, transmission, use and disclosure of personal information.").

153. *See supra* notes 121-23 and accompanying text.

154. *See, e.g., supra* notes 107-12 and accompanying text.

155. *See supra* note 107.

156. *See West's Legal News 96*, Jan. 11, 1996, *available in* 1996 WL 257854; *see also* Prowda, *supra* note 64, at 761.

157. *See* Medical Records Confidentiality Act, *supra* note 107 § 203(e). Patient consent before disclosure is not required in the following instances: when creating nonidentifiable information for a health information service (§ 204); when releasing information to patient's next of kin (§ 205); in emergencies (§ 206); when releasing information to oversight committees (§ 207); when releasing information for public health reasons (§ 208); when releasing information for health research (§ 209); when releasing information for judicial and administrative purposes (§ 210); when releasing information for non-law enforcement subpoenas (§ 211); and when releasing information for law enforcement purposes (§ 212). *See* Beverly Woodward, *Patients' Privacy at Risk*, N.Y. TIMES, Nov. 15, 1995, at A23.

158. *See* THE HEALTH LAW HANDBOOK 400-01 (Alice G. Gosfield ed., 1996).

standard. Telemedicine patients with certain conditions may be guaranteed privacy protection, while others may be ignored and left vulnerable to wrongful disclosure.

The Uniform Health-Care Information Act[159] has been adopted by only two states and also provides numerous exceptions to the patient consent requirement before disclosure.[160] In addition, each state can make changes to the law before adoption,[161] perpetuating the current scheme of varying laws from state to state.

The Model Act proposed by the Federation of State Medical Boards[162] is inadequate because it fails to establish a universal standard for patients in all states. The Act applies only confidentiality laws of the state in which the act is passed. As a result, patients in differing states will still be subject to varying protections. Furthermore, the act provides sanctions only for those physicians who practice medicine in another state without being licensed in that state.[163] The act mentions no available sanctions against those who make unauthorized disclosures.

E. Proposal: The Need for Model Federal Legislation

Today's privacy laws provide inconsistent and inadequate protection for patient health information. Because of broad access capabilities to electronically transmitted medical data, telemedicine patients are left particularly vulnerable. As a result, uniform federal legislation is necessary to protect the confidentiality of telemedicine patients' medical information.[164] To most effectively safeguard against unauthorized and inappropriate disclosure of electronic medical data, federal legislation must be comprehensive, filling the loopholes that other privacy protection attempts have left open.

First, the law must apply to both government *and* private actors. Current federal privacy laws ignore that private parties handle the

159. *See* Unif. Health-Care Information Act, *supra* note 113 and accompanying text.

160. *See id.* § 2-104. Disclosure without authorization is permitted in nine situations, including disclosure to health-care providers for treatment (§ 2-104(a)(1)) or education purposes (§ 2-104(a)(2)); to immediate family members (§ 2-104(a)(5)); to researchers (§ 2-104(a)(7)); and to penal institution officials (§ 2-104(a)(9)).

161. *See* Schwartz, *supra* note 58, at 322.

162. *See* Model Act, *supra* notes 116-17.

163. *See id.*

164. Such federal legislation regulating private actors in the practice of interstate telemedicine may be justified under Congress' commerce clause authority. *See* U.S. v. Lopez, 514 U.S. 549, 560 (1995) ("Where economic activity substantially affects interstate commerce, legislation regulating that activity will be sustained.").

majority of patient medical information.[165] Legislation must specifically apply to doctors, administrators, office workers and clerks, insurers, researchers, and all others who access, use, and maintain personal health information. These individuals must be bound by a code of ethics similar to the physicians' oaths developed by Hippocrates[166] and the American Medical Association.[167] All medical and non-medical personnel, from doctors to administrators, must receive training about the heightened risks involved in electronic records, the highly sensitive nature of patient health information, the dangers inherent in improper disclosure,[168] and the necessity of obtaining the patient's informed consent for disclosure. They should sign confidentiality clauses outlining their duty of privacy to their patients.[169]

The federal law must also codify and elaborate on the principles of fair information practices.[170] These principles include that: (1) information should be collected only for the purpose for which it is intended; (2) information should not be used for a different purpose without the patient's consent; (3) information should be discarded when it is no longer needed to fulfill that purpose; and (4) individuals should be informed of how the information will be used.[171]

The first, second, and fourth principles indicate that federal legislation must set forth a scheme of informed consent, where the physician educates the patient about his or her rights to prevent disclosure of private medical images and data and the potential risks of disclosure. Some telemedicine providers have already used this practice.[172] The consent form must clearly detail the intended use of the information and must inform the patient of exactly who

165. *See supra* notes 142-44 and accompanying text.

166. *See supra* note 55 and accompanying text.

167. *See id.* and accompanying text.

168. *See* Francoise Gilbert, *How to Minimize the Risk of Disclosure of Patient Information Used in Telemedicine*, 1 TELEMEDICINE J. 91, 93 (1995).

169. *See id.* The duty should consist of a promise to use patient information for intended purposes only, and to obtain patient consent before releasing such data to a third party. *Id.* at 93.

170. The Federal Privacy Act of 1974 was based upon these principles. *See* Gostin, *supra* note 20, at 25. The Secretary's Advisory Committee on Automated Personal Data Systems developed these principles in 1972 in reaction to individuals' lack of control over records containing their personal information. *See* Community Health Management Information Systems Resource Center, *Primer on Privacy* (visited Sept. 26, 1996) <http://chmis.org/>.

171. *See* Gostin, *supra* note 20, at 25.

172. *See* Bradham, *supra* note 2, at 166 n.63 ("Some telemedical practitioners require their patients to sign a 'statement of understanding for videoconsultations.'")

will have access to his or her health information.[173] The patient must be informed of the risks of disclosure in telemedicine practice before the telemedical consultation begins. The consent form must also outline the patient's legal recourse, should his or her confidentiality be breached.

The third principle requires the development of explicit provisions for the destruction of data used in telemedicine.[174] Once the original purpose of obtaining the information is attained, all transmitted data must be completely erased. This would eliminate the possibility of a subsequent breach of the patient's privacy.

In addition, strong security safeguards, such as encryption,[175] password programs, and handprint recognition and retina scanning technologies,[176] must be required to prevent unauthorized outsider and insider access.[177] Telemedicine providers should be required to use protections equal to the "state of commercially available technology."[178] A monitoring system must be created to ensure that telemedicine providers are adequately protecting their patients'

(citation omitted); *see also supra* note 132 and accompanying text (discussing the informed consent requirement of California's Telemedicine Development Act of 1996).

173. This system has proven successful for at least one hospital. Employees are told that "all patients will receive a list of all employees that had access to their medical records. The move has resulted in much less voyeurism among employees . . . ." *See* McCormack, *supra* note 23.

174. *See, e.g.*, Gilbert, *supra* note 168, at 93-94. Destroying the images and text sent between locations should not violate state medical records retention laws, because the originals would continue to be maintained by the referring physician.

175. Encryption "protect[s] digital information by scrambling data using mathematical procedures that make it extremely difficult and time-consuming for anyone other than authorized recipients . . . to recover the plain text of the message. 'Strong' encryption . . . guarantees that the information will be safe even if it falls into hostile hands." Conrad Burns, *Development of Internet Services Hurt by Export Encryption Policy*, N.Y. L.J., Oct. 15, 1996, at 5.

176. These technologies "store images of the unique identifying parts of the human hand or eye so a system later can identify [authorized] computer or network users." *Addressing Security in the Networking Era*, HEALTH DATA MGMT., Nov. 1, 1996, *available in* 1996 WL 9609831.

177. It is true, however, that some current safeguards do not always offer sufficient protection. *See* Hanzal, *supra* note 1, at 5. Yet without some form of effective encryption, "medical information is readily available to anyone interested in obtaining it." *On-Line Security Issues, 1996: Hearings Before Subcomm. on Science, Technology and Space of the Comm. on Commerce, Science, and Transportation*, (June 26, 1996) (statement of Robert G. Gargus, President, Atalla), *available in* 1996 WL 10829264.

178. The Health Law Resource, *American Health Information Management Association Language for Model Health Information Legislation on Creation, Authentication and Retention of Computer-Based Patient Records* (visited Sept. 26, 1996) <http://www.netreach.net/~wmanning>. Generally, longer mathematical formulas with no "back doors," or ways for insiders (or hackers) to bypass a system's normal login procedure, provide the greatest encryption protection. Burns, *supra* note 175, at 5.

confidentiality. Policing duties may be assigned to hospital institutional review boards ("IRBs"), which are already experienced in safeguarding patients' privacy.[179]

Finally, legislation must establish strong penalties for the unauthorized disclosure or misuse of patient information. The stringent civil and criminal sanctions of the proposed Medical Records Confidentiality Act of 1995, which provide for penalties up of to $500,000 and 10 years in prison, may serve as a model.[180]

Federal legislation is the best alternative to safeguard patients' medical information used in telemedicine. It is not, however, foolproof. No matter what procedures are required by law, the confidentiality of patient data cannot be guaranteed one hundred percent.[181] Health care personnel may defy their duties and continue to carelessly or intentionally invade their patients' right to privacy.[182] Hackers may elude security mechanisms in place.[183] Some groups may even prefer to leave strong state laws in place over a diluted federal protection.[184] Federal legislation, however, is a good beginning, taking steps to uniformly protect the confidentiality of patient medical information transmitted by telemedicine.

Conclusion

Current laws have not kept pace with emerging telemedicine technology. Federal laws are inadequate in protecting patients' medical privacy. State laws provide inconsistent and conflicting standards of patient confidentiality protection. As a result, telemedicine patients are exposed to abuse and misuse of their private health information. The consequences of maintaining the status quo are enormous: telemedicine will be stifled, access to

179. *See* Duncan Neuhauser, Comment, *More Tales From Institutional Review Boards*, 4 HEALTH MATRIX 153, 154 (1994). IRBs review institutional research projects to ensure that participating patients are protected via informed consent and confidentiality safeguards. *Id.*

180. *See supra* note 110 and accompanying text.

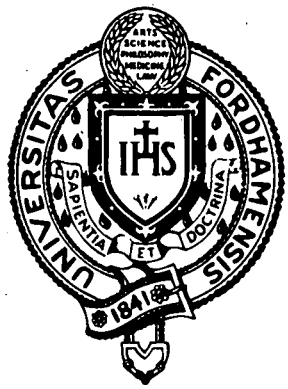
181. *See* HEALTH DATA MGMT., *supra* note 176 ("There is no silver bullet to security issues . . . . Protecting health data and networks is a combination of doing many different things. But even then, you do not have absolute insurance.") (quoting William M. Miaoulis, an information security officer at the University of Alabama Hospital).

182. *See supra* notes 61-63 and accompanying text.

183. *See supra* note 60 and accompanying text.

184. Some AIDS advocates, for example, would rather have a federal standard preempt just *weak* state confidentiality laws than preempt *all* state confidentiality laws. Lavelle, *supra* note 122, at A1 (emphasis added). For example, AIDS patients in California are given strict protection that a federal law might not be able to duplicate. *See, e.g.*, *supra* note 124 (citing California HIV privacy law).

affordable primary and specialist care will be denied, lives will be lost, money will be wasted, and rights will be violated. The best solution is a comprehensive, national privacy protection law that guarantees all telemedicine patients the same confidentiality standard. Only then will the law allow patients sufficient safeguards to take advantage of the new frontier of telemedicine.


ARTS
SCIENCE
PHILOSOPHY
MEDICINE
LAW
UNIVERSITAS FORDHAMENSIS
IHS
SAPIENTIA ET DOCTRINA
1841