North Dakota Law Review

Volume 76 | Number 2 Article 3

2000

Virual Web Wave of the Future: Integration of Healthcare Systems on the Internet

Barbara J. Williams

VIRTUAL WEB WAVE OF THE FUTURE: INTEGRATION OF HEALTHCARE SYSTEMS ON THE INTERNET

BARBARA J. WILLIAMS*

I. INTRODUCTION

The medical community has not been quick to use computers.[1] In comparison with banks, which spend seven percent of their annual revenues on information systems, the healthcare industry spends only one to two percent for this purpose.[2] Analyst Stephen Savas of Goldman Sachs considers the healthcare industry to be ten to fifteen years behind the times.[3]

However, the situation is quickly changing, and the healthcare industry is embracing newly emerging medical integrated information systems.[4] For example, HBOC, a healthcare information technology company with systems in 9,000 hospitals, doctor's offices, and managed care companies, has strategically increased its holdings by $2.1 billion through the acquisitions of rivals and integration of their niche products into HBOC's own system.[5] In addition, Lucent Technologies has joined in a new venture with HealthCenter Internet Services Inc. to utilize the Internet to deliver patient medical records management, test report transmission, chronic disease management, telemedicine and remote monitoring.[6]

Why are companies aggressively pursuing such integration? "The healthcare industry has never been more dependent on timely, effective communication."[7] The Department of Health and Human Services estimates that healthcare providers could save more than $100 billion with an information network.[8] In addition, information is potentially very profitable for the companies involved; healthcare information technology is estimated to become a $26 billion industry by 2002.[9]

---

* Barbara J. Williams is an LL.M. candidate at the University of Houston Law Center. She is a member of the bar in the states of New York, New Jersey and Texas.

1. *See Hardly Wired,* ECONOMIST, Oct. 24, 1998, at 68.
2. *See id.*
3. *See id.*
4. *See id.* (stating that the healthcare industry is "rushing to catch up").
5. *See id.*
6. *See* Lucent Technologies, *New Lucent Technologies Venture with HealthCenter Internet Services to Develop Highly Secure Infrastructure for Health Care Providers* (June 27, 2000) (press release), *available at* <www.lucent.com/press/0600/000627.coa.html>.
7. James Gifford, *Communications Rx: CT for Healthcare,* COMPUTER TELEPHONY, June 2000, at 114.
8. *See Hardly Wired, supra* note 1, at 68.
9. *See id.*

II. ADVANTAGES OF AN INTEGRATED SYSTEM

Healtheon/WebMD (WebMD) is one example of an innovative company attempting to bring together the information systems in the healthcare industry. It has described itself as the first end-to-end provider of healthcare information and services.[10] With the development of a secure Internet connection accessed through the World Wide Web, WebMD hopes to simplify workflows, decrease costs, and improve the quality of patient care.[11] This secure Internet connection enables the exchange of information among a wide array of disparate healthcare systems and provides a framework for a broad range of healthcare transactions.[12]

WebMD's Benefit Central allows employees to compare company sponsored plans and other benefits, search provider directories, and electronically enroll for benefits.[13] WebMD Practice permits a physician's office staff to establish, search for, and view a patient roster[14] and determine patient benefit eligibility.[15] A virtual receptionist[16] or answering service[17] may be utilized. The patient may store medical records with WebMD.[18] After examination of the patient, the medical provider may answer questions about diagnosis or treatment by logging onto the medical library.[19] A physician may order laboratory tests[20] or prescriptions[21] via the secure Internet connection and laboratory reports may also be received. New patient referrals may be made or existing referrals of the patient may be checked.[22] WebMD Practice also

---

10. *See* Healtheon Corporation, *Healtheon to Provide E-Commerce Services to LabCorp* (Aug. 31, 1999) (press release), *available at* <http://www.healtheon.com/news/pr_08_31_99.html>.

11. *See* Healtheon Corporation, *Quarterly Report Pursuant to Section 13 or 15(d) of the Securities and Exchange Act of 1934 for the Period Ended June 30, 1999*, *available at* <http://www.sec.gov/Archives/edgar/data/1009575/0000891618-99-003789.txt>.

12. *See id.*

13. *See WebMD Health [Benefit Central]* <http://www.my.webmd.com/benefit_central>.

14. *See WebMD Practice, Patient Search, Create Patient Roster, View Patient Roster* <http://webmd-practice.medcast.com/Z/Channels/3152/temp.html>.

15. *See WebMD Practice, Check Eligibility* <http://webmd-practice.medcast.com/Z/Channels/2840/lookup.html>.

16. *See WebMD Practice, Virtual Receptionist* <http://webmd-practice.medcast.com/Z/Channels/2838/virtualreceptionist.html>.

17. *See WebMD Practice, WebMD OnCall Answering Service* <http://webmd-practice.medcast.com/ Z/Channels/2854>.

18. *See WebMD Health: What is my Health Record?* <http://webmd.com/my_health_record>.

19. *See WebMD Health* <http://my.webmd.com>.

20. *See WebMD Practice, Laboratory Reports* <http://webmd-practice.medcast.com/Z/Channels/2839/lablist.html>.

21. *See WebMD Practice, Rx Services* <http://webmd-practice.medcast.com/Z/Channels/3153/rntemp.html>.

22. *See WebMD Practice, New Referrals, Check Referrals* < http://webmd-practice.medcast.com/Z/Channels/2840/checkref.html>.

provides dictation and transcription services over the Internet for the provider to update a patient's medical record.[23] The fee to be charged can be compared with the WebMD Practice data bases of physician fees[24] and the coding of the services checked against the Medicare Correct Coding Initiative, local Medicare Review Policies and proprietary alerts, as a precaution against Medicare fraud and abuse.[25] In addition, the insurance claim can be checked[26] and sent[27] through the WebMD Practice system.

By having all transactions go through the secure Internet connection via the World Wide Web, it is possible for various aspects of the healthcare system to communicate with each other without the cost of networking, systems integration or custom programming.[28] This considerably reduces costs to make use by the small provider and hospital economically practical.[29] In essence, a virtual Internet health maintenance organization has been created.[30]

There are many other uses of electronic information systems in healthcare. Electronically stored medical records would increase the use of telemedicine for worldwide medical consultations.[31] Physicians could continually access updated physiological data about critical care patients from remote locations.[32] In an attempt to increase the healthcare

---

23. *See WebMD Practice, Dictation and Transcription Services* <http://webmd-practice.medcast.com/Z/Channels/2838/dictationtranscription.html>.

24. *See WebMD Practice, Fee Schedule Analyzer* <http://webmd-practice.medcast.com/Z/Channels/2838/feeschedule.html>.

25. *See WebMD Practice, Coding Compliance Monitor* <http://webmd-practice.medcast.com/Z/Channels/2838/codingcompliance.html>.

26. *See WebMD Practice, Check Claims* <http://webmd-practice.medcast.com/Z/Channels/2840/checkclaim.html>.

27. *See WebMD Practice, Send Claims* <http://webmd-practice.medcast.com/Z/Channels/2840/sendclaims.html>.

28. *See Solutions for Physicians.Hospitals.Medical Groups* <http://www.healtheon.com/phys/index.html> (advertising Healtheon as a "low cost means of managing information and workflows, automating complex administrative and care management functions of physician practices and managed care" via the Internet).

29. *See id.*

30. *See* Todd Woody, *Health Care for the Wired and Uninsured*, INDUSTRY STANDARD, Oct. 11, 1999, at 47 (explaining how Healtheon and Alternative Technology Resources hope to give uninsured patients access to doctors providing discounted medical services if those patients schedule appointments online).

31. *See* Edward Ericson, Jr., *Decisions, Decisions: How Computer Programs Control Your Health Care*, FAIRFIELD COUNTY W KLY., Oct. 24, 1999, at 15 (stating that the broad electronic access to patient medical records is important for telemedicine). Telemedicine is defined as "the use of telecommunication [as opposed to face-to-face contact] to treat a patient." Patricia C. Kuszler, *Telemedicine and Integrated Health Care Delivery: Compounding Malpractice Liability*, 25 AM. J. L. & MED. 297, 299 (1999); *see also* Rashid L. Bashshur, *On the Definition and Evaluation of Telemedicine*, 1 TELEMEDICINE J. 19 (1995).

32. *See generally* Valeriv Nenov & John Klopp, *Remote Analysis of Physiological Data from Neurosurgical ICU Patients*, 3 J. AM. MED. INFORMATICS ASS'N 318 (1996) (describing a system developed by the UCLA Neurosurgery Intensive Care Unit to access medical information over the World Wide Web).

opportunities for the uninsured, WebMD and Alternative Technology Resources have entered into a joint venture to create a system for uninsured consumers to schedule appointments with physicians and pay for services with credit cards.[33] The physicians, usually those not associated with health maintenance organizations or managed care organizations, would give the consumers discounts of fifteen to fifty percent.[34] Another example of healthcare via the Internet is AmericasDoctor.com, which allows "guests" to ask physicians questions over the Web.[35] The answers are characterized as "information" not medical advice.[36]

Physician WebLink has developed another electronic information innovation through a virtual chart which allow a physician to enter patient information electronically, thus totally eliminating a paper chart.[37] IMPACT.MD, an imaging software developed by Advanced Imaging Concepts Incorporated could handle all of the paperwork associated with billing and permit a provider's office staff to scan charts into the computer.[38] Additional uses for the Web in healthcare, while sometimes bizarre, are developing daily.[39]

Individuals in the industry consider an integrated system to have many values aside from administrative efficiency.[40] For example, computerized records would allow "decision support."[41] Decision support on a "micro" level would allow a doctor to know immediately what medications a patient is taking.[42] On a "macro level" it could allow researchers to combine data in cancer cases to determine the optimum level of cancer and radiation therapy.[43]

Electronic medical records could also save valuable time in emergency situations in remote portions of the world where medical information would otherwise be inaccessible. In addition, consumers will be able to make better choices about health plans, providers, diagnoses and treatments.[44] Healthcare services fraud and abuse could be more

33. *See* Woody, *supra* note 30, at 47.

34. *See* Woody, *supra* note 30, at 47.

35. *See* David Brown, *Log On and Say 'Ahhh' Online Doctor Visits are Uncharted Territory*, WASH. POST, Aug. 22, 1999, at A1.

36. *See id.*

37. *See* Harold J. Adams, *Electronic Healing*, COURIER-JOURNAL (Louisville, Ky), July 2, 2000, at E1.

38. *See id.*

39. For instance, one human kidney was for sale at a price which rose to $5.7 million before the solicitation was pulled by eBay. *See* Amy Harmon, *Auction for Kidney Pops Up on eBay's Site*, N.Y. TIMES, Sept. 3, 1999, at A13.

40. *See* Ericson, *supra* note 31.

41. *See* Ericson, *supra* note 31.

42. *See* Ericson, *supra* note 31.

43. *See* Ericson, *supra* note 31 (describing a database used to research common diseases).

44. *See* James G. Hodge, Jr. et al., *Legal Issues Concerning Electronic Health Information: Privacy, Quality and Liability*, 282 JAMA 1466, 1466 (1999).

effectively monitored.[45] Public health morbidity and mortality information across populations could also be gathered.[46]

III. PRIVACY CONCERNS

But such innovation is not without problems. One of the main issues involved with such a system is maintaining patient medical record privacy. The public is concerned with this issue.[47] Their concerns are compounded by horror stories of leaks of patient medical information over the Web and elsewhere.[48] The public is also concerned that their patient medical information may travel to third parties without their consent.[49] Patients fear not only losing control of their medical information,[50] but they also fear the adverse consequences that may result from deliberate or inadvertent disclosure to employers[51] and insurance companies.[52]

Unauthorized and unintentional disclosure indicate the public's fears are not unwarranted.[53] With little more than basic information

---

45. *See id.* at 1466-67.

46. *See id.* at 1466.

47. The Wall Street Journal and NBC News took a poll about concerns for the next century. *See* Christy Harvey, *Breakthroughs in Medicine, Technology Are Forecast; But the Auto is Still Here*, WALL ST. J., Sept. 16, 1999, at A10. Twenty-nine percent stated their main concern was loss of personal privacy. *See id.* Issues such as terrorism, world war, and global warming had scores of 23% or less. *See id.* In a recent survey, 75% of internet users were "concerned" or "very concerned" that information provided to an internet health site would be shared without permission with third parties. *See* CALIFORNIA HEALTHCARE FOUNDATION, ETHICS SURVEY OF CONSUMER ATTITUDES ABOUT HEALTH WEB SITES 3 (1999), *available at* <http://admin.chcf.org/documents/ehealth/ surveyreport.pdf>. More disturbing is the fact that one-sixth of those who access health sites are providing inaccurate information, changing doctors frequently or not getting care in an effort to thwart their concerns of invasion of privacy. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,920 (1999) (to be codified at 45 C.F.R. pts. 160-64).

48. *See* Lauren Weinstein, *Confidential Patient Data Accidentally Released to the Web*, 8 PRIVACY F. DIG. (online magazine) <http://gopher.vortex.com/privacy/priv.08.04> (reporting a situation involving public access to University of Michigan patient records and describing how this access was discovered and controlled).

49. *See generally* Ericson, *supra* note 31. Currently 20 million medical files are housed on computers by Medical Information Bureau in Westwood Massachusetts and these files are available in real time to any of the 600 insurance companies that pay for their upkeep and contribute data. *See* Ericson, *supra* note 31. The insurance companies use the data to detect fraud and evaluate the risk of applicants for insurance policies. *See* Ericson, *supra* note 31.

50. *See generally* LAWRENCE O. GOSTIN, LEGISLATIVE SURVEY OF STATE CONFIDENTIALITY LAWS WITH SPECIFIC EMPHASIS ON HIV AND IMMUNIZATION (Feb. 1997), *available at* <http://www.epic.org/ privacy/medical/cdc_survey.html>.

51. *See* Ericson, *supra* note 31. The Survey Research Laboratory at the University of Illinois found that one third of the Fortune 500 companies made hiring, firing and promotional decisions using medical information. *See* Ericson, *supra* note 31, at 17.

52. *See* Ericson, *supra* note 31 (stating that it is possible to ration the level of care by using composite computerized data while shielding the insurer from liability).

53. *See* Robert O'Harrow, Jr., *Fearing a Plague of 'Web Bugs': Invisible Fact-Gathering Code Raises Privacy Concerns*, WASH. POST, Nov. 13, 1999, at E1 (describing how "Web Bugs" allow a company to fetch data from web sites without a computer user's knowledge and send it to databases for analysis and storage).

about a person, detailed medical profiles can be established using online networks, Internet chat boards and retrieval services.[54] Yet companies offering healthcare information services over the Internet contend that healthcare participants must allow sensitive information to be stored in their databases; if not, the benefits of their connected and sophisticated information system would be limited under these circumstances.

IV. METHODS TO PROTECT PRIVACY

On a global scale, the World Wide Web Consortium (W3C)'s Platform for Privacy Preferences (P3P)'s goal is to (1) allow the user to interact with web sites with privacy practices acceptable to the user, (2) allow the user to delegate the privacy decisions to a computer agent, and (3) tailor interaction with specific site for future use.[55] For example, an insurer could send a proposal for research using personally identifiable information of the patient along with the privacy practices it would expect from the web site.[56] The privacy practices detail the data elements that would be collected, how each would be used, with whom the data would be shared, and whether data would be used in an identifiable manner.[57] A user agent, such as Netscape, would compare the privacy preferences of the site with the preferences of the user. If the preferences match, use of the site commences.[58] If the preferences do not match, the insurer would be required to send back other proposals until a "match" is created.[59]

This process is called privacy "negotiation."[60] Rather than requiring a user to send new proposals with every contact, a service could merely confirm the existence of a previous agreement with a digital signature of the user.[61] To ensure the site lives up to its agreement, online organizations take action against a service provider that violates the agreement.[62] However, while this mechanism would only increase the *information* and *control* the users have concerning the degree of privacy applicable to the information provided, it would not make that

54. *See* Hodge, *supra* note 44, at 1467.

55. *See* Joseph Reagle & Lorrie Faith Cranor, *The Platform for Privacy Preferences* <http://www.w3.org/ TR/1998/NOTE-P3P-CACM-19981106/>.

56. *See id.*

57. *See id.*

58. *See id.*

59. *See id.*

60. *See id.*

61. *See id.*

62. *See* Alex Lash, *Privacy, Practically Speaking*, INDUSTRY STANDARD, July 23, 1999 (online article) <http://www.thestandard.com/article/display/0,1151,5613,00.html)>.

information more secure against access and unauthorized use by outsiders.[63]

V. METHODS TO PREVENT UNAUTHORIZED ACCESS OR USE

The American Medical Association (AMA) is currently issuing "digital credentials" for physicians accessing information, such as patient test results, over the Internet.[64] Partnering with Intel, the AMA will create digital credentials of encrypted software that will verify the identity of users who access web sites.[65] This information will insure that only authorized physicians, insurers, and consumers can access a patient's medical transcripts and other medical records.[66]

Another company, PersonalMD.com allows patients to keep their medical records online in a secure database that is only accessible to physicians and users themselves.[67] By August of 1999, over 30,000 patients had transferred their records to the data warehouse.[68] When patients become part of the system, they signed a disclaimer permitting emergency room physicians immediate access to the records.[69] This permits instantaneous access to vital information.[70]

An international project, "Health on the Net" provides guidelines for encryption.[71] Worldtalk Corporation has established a WorldSecure Server that helps organizations provide legally required security by encrypting the data before it is transmitted over the Internet.[72] Additionally, the server provides content filtering that can prevent certain

---

63. *See* Karen Coyle, *Some Frequently Asked Questions About Data Privacy and P3P* <http://cpsr.program/privacy/p3p-faq.html>.

64. *See* Charles Piller, *Technology Briefs: AMA to Credential Web MDs*, LOS ANGELES TIMES, Oct. 12, 1999, at C3.

65. *See id.*

66. *See id.*

67. *See* Matt Villano, *Finding a Market in Online Medical Data*, BOSTON GLOBE, Aug. 9, 1999, at C3.

68. *See id.*

69. *See id.*

70. *See id.*

71. *See About Health on the Net Foundation* (last modified Mar. 29, 2000) <http://www.hon.ch/Global/about_HON.html>.

72. *See WorldSecure and the Healthcare Industry: Security Solutions to Protect Patient Privacy* <http://www.securtekcorporation.com/Download/WSShcbr.pdf> [hereinafter *WorldSecure*]. The Health Care Financing Administration's (HCFA) Internet Security Policy states:

> It is permissible to use the Internet for transmission of HCFA Privacy Act-protected and/or other sensitive HCFA information, as long as an acceptable method of encryption is utilized to provide the confidentiality and integrity of this data, and that authentication or identification procedures are employed . . . .

HCFA Internet Security Policy (last updated Feb. 19, 1999) <www.hcfa.gov/security/isecplcy.htm>; *see also* Beverly Kane & Daniel Z. Sands, *Guidelines for the Clinical Use of Electronic Mail with Patients*, 5 J. AM. MED. INFORMATICS ASS'N 104, 109 (1998) ("As soon as practicable, clinics should establish a means of secure communication using data encryption methods . . . .").

documents, such as patient records, from leaving the organization unless proper steps have been taken to protect confidentiality.[73] The company also can provide this security on a network integrated system-wide basis with firewalls so that data will not be mistakenly shared.[74]

VI. THE STATE OF THE LAW REGARDING THE PRIVACY CONCERNS CREATED BY MEDICAL INTEGRATED SYSTEMS

The Supreme Court's crystal ball foresaw that the accumulation of personal data by organizations, such as medical integrated systems, could become an issue the Court would need to address.[75] In *Whalen v. Roe,*[76] the Supreme Court left the issue open:

> A final word about the issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The . . . supervision of public health . . . require[s] the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. . . . We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions.[77]

In his concurring opinion, Justice Brennan also reserved analysis of this issue: "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

---

73. *See WorldSecure, supra* note 72.

74. *See WorldSecure, supra* note 72. A "firewall" is a specially designed device that controls the spread of a network threat. *See FishNet Security* <http:www.fishnetsecurity.com/secinfo/overview.html>. A firewall consists of a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. *See id.* The term can also refer to the security policy that is used with the programs. *See Firewall* <http://www.whatis.com/firewall.htm> ("An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and [to] control[ ] what outside resources its own users have access to.").

75. *See* Whalen v. Roe, 429 U.S. 589, 605-06 (1977).

76. 429 U.S. 589 (1977).

77. *Whalen*, 429 U.S. at 605-06 (citing Barry B. Boyer, *Computerized Medical Records and the Right to Privacy: The Emerging Federal Response*, 25 BUFF. L. REV. 37 (1975); Arthur R. Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUM. RTS. L. REV. 1 (1972); ARTHUR R. MILLER, THE ASSAULT ON PRIVACY (1971)).

necessity of some curb on such technology."[78] Justice Stewart also wrote a concurring opinion and stated that he would have left the issue for resolution by the states.[79]

At the present time, privacy law is an inadequate "patchwork" of provisions.[80] Constitutional protections extend only to the activities of the government, not to the private entities where most of the electronic information is being disseminated.[81] The same is also true of the Federal Privacy Act of 1974[82] and the Freedom of Information Act of 1966,[83] which apply only to governmental activities. The Electronic Communications Privacy Act made it unlawful to intentionally intercept the contents of an electronic communication such as e-mail.[84] In 1996, patient privacy protection was included in the Consumer Bill of Rights and Responsibilities created by the President's Advisory Commission on Consumer Protection and Quality Care in the Health Care Industry.[85] Other federal laws protect patient privacy in narrow and limited circumstances.[86]

The Health Insurance Portability and Accountability Act of 1996[87] (HIPAA) required the Department of Health and Human Services to send recommendations for protecting healthcare information to Congress.[88] The Department of Health and Human Services did so in 1997.[89] HIPAA also required the Department of Health and Human Services to develop standards to protect the security, confidentiality and integrity of health information. Many of these standards have been

---

78. *Id.* at 607 (Brennan, J., concurring).

79. *See id.* at 608 (Stewart, J., concurring).

80. *See* Hodge, *supra* note 44, at 1468.

81. *See* Hodge, *supra* note 44, at 1468.

82. *See* Hodge, *supra* note 44, at 1468 (citing Federal Privacy Act of 1974, 5 U.S.C. § 552(b)(1)-(3), (6) (1994)).

83. *See* Hodge, *supra* note 44, at 1468 (citing Freedom of Information Act of 1966, 5 U.S.C. § 552 (1994 & Supp. IV 1998)).

84. *See* 18 U.S.C. § 2511 (1994 & Supp. IV 1998). Currently, e-mail communication between physicians and their patients is limited by malpractice and security concerns. *See* John R. Washlick & Elaina R. Cohen, *The Brave New World of Internet Telemedicine*, N.J. L.J., Dec. 13, 1999, at 33.

85. *See* PRESIDENT'S ADVISORY COMMISSION ON CONSUMER PROTECTION AND QUALITY IN THE HEALTH CARE INDUSTRY, Strengthening the Market to Improve Quality ch. 9, *available at* <http://www.hcqualitycommission.gov/final/chap09.html>.

86. *See* Hodge, *supra* note 44, at 1468 (citing Americans with Disabilities Act, 42 U.S.C. § 12112(d)(3)(B) (1994); Public Health Service Act, 42 U.S.C. §§ 241(d), 290dd-2 (1994); Federal Policy for Protection of Human Subjects, 45 C.F.R. § 46.101-46.404 (1996); Medicare Conditions of Participation, 56 Fed. Reg. 28,003 (1991)).

87. Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of U.S.C.).

88. *See* 42 U.S.C. § 1320d-2 note (Recommendation with Respect to Privacy of Certain Health Information) (Supp. IV 1998).

89. *See* SECRETARY OF HEALTH AND HUMAN SERVICES, CONFIDENTIALITY OF INDIVIDUALLY-IDENTIFIABLE HEALTH INFORMATION (1997), *available at* <http://aspe.hhs.gov/admnsimp/pvcrec.htm>.

issued as proposed regulation but have not been promulgated in final form.[90]

These standards are known as the Administrative Simplification Provisions ("Provisions").[91] These Provisions propose uniform standards for electronic exchange of health information in administrative and financial transactions, and data elements for such transactions.[92] Under HIPAA, the Department of Health and Human Services must also promulgate standards for unique health identifiers for each individual employer, health plan, and health providers, as well as security standards and safeguards for health information.[93] In conjunction with the Secretary of Commerce, HIPAA also requires the Secretary of the Department of Health and Human Services to adopt provisions with electronic signature standards for the transmission and authentication of signatures for these transactions.[94] The Provisions apply to all health plans, healthcare clearinghouses, and healthcare providers who transmit information electronically.[95] The main goal of the Provisions is to establish standards in electronic healthcare transactions[96] "for reducing the administrative costs of providing and paying for healthcare."[97]

Additionally, the Provisions contain sections relating to privacy[98] of healthcare information. Compliance is required two years after the enactment of each standard or three years for small health plans.[99] There are Provisions containing monetary penalties for violations of the general Provisions.[100] There are also specific, and very tough, criminal and

---

90. *See* Department of Health and Human Services, *Tentative Schedule for Publication in HIPAA Administrative Simplification Regulations* <http://aspe.os.dhhs.gov/admnsimp/pubsched.htm>.

91. *See* 42 U.S.C. §§ 1320d to 1320d-8 (Supp. IV 1998).

92. *See id.* § 1320d-2.

93. *See id.* § 1320d-2(b), (d).

94. *See id.* § 1320d-2(e).

95. *See* 42 U.S.C. § 1320d-1(a).

96. *See* 42 U.S.C. § 1320d-2(a)(1). A transaction means any of the following:

(A) Health claims or equivalent encounter information.
(B) Health claims attachments.
(C) Enrollment and disenrollment in a health plan.
(D) Eligibility for a health plan.
(E) Healthcare payment and remittance advice.
(F) Health plan premium payments.
(G) First report of injury.
(H) Health claim status attachments.
(I) Referral certification and authorization.

42 U.S.C. § 1320d-2(a)(2).

97. 42 U.S.C. § 1320d-1(b).

98. *See* 42 U.S.C. § 1320d-2 note (Recommendations with Respect to Privacy of Certain Health Information).

99. *See* 42 U.S.C. § 1320d-4(b). Small health plans are defined in the regulations as health plans with annual receipts of $5 million or less. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,932 (1999) (to be codified at 45 C.F.R. pts. 160-64).

100. *See* 42 U.S.C. § 1320d-5. Penalties may not be more than $100 per person per violation and

monetary penalties for disclosing health identifiers or obtaining or disclosing individually identifiable health information.[101]

The House version[102] of a recently passed banking reform bill contained a provision, that would have allowed health insurance companies to disclose individual medical records to banks even though the bill was characterized as a medical confidentiality provision.[103] The provision would have "allow[ed] broad disclosures of private medical information without a patient's permission."[104] The legislation would have allowed insurance companies to release such information for many purposes including determining charges for premiums, medical research, and other research.[105] Banks and credit card companies were among the allowable recipients and no restrictions were placed on the use of the information.[106] The medical sharing provisions were dropped from the compromise bill at White House request.[107] Since the two sides could not agree, Congress put off the issue for future consideration.[108]

The legislation that finally emerged from Congress, the Gramm-Leach-Bliley Financial Modernization Act of 1999,[109] prohibited financial institutions from disclosing personally identifiable information to nonaffiliated third parties.[110] It contains no restrictions to prevent financial institutions from sharing information with *affiliated* parties.[111] Instead, Congress proposed the that Department of the Treasury and the Federal Trade Commission study the sharing of information among financial institutions and their affiliates and report back in the year 2002.[112] Because an insurance company could be an affiliate as defined

---

not more than $25,000 per person for violations of a single standard for a calendar year. *See* 42 U.S.C. § 1320d–5(a)(1).

101. *See* 42 U.S.C. § 1320d-6. The penalties include: (1) A fine of not more than $50,000 and/or imprisonment for not more than one year; (2) if the offense is "under false pretenses," a fine of not more than $100,000 or imprisonment of not more than five years; and (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years. *See id.*

102. *See* H.R. 10, 106th Cong. § 178 (1999).

103. *See* Alissa J. Rubin, *House Approves Disclosure of Private Medical Records*, LOS ANGELES TIMES, July 2, 1999, at A1.

104. *Id.*

105. *See id.*

106. *See id.*

107. *See* Committee on Banking and Financial Services, *Leach Introduces Medical Financial Records Privacy Bill* (June 6, 1999) (press release) [hereinafter Leach press release], *available at* <http://www.house.gov/banking/6600pr.htm>.

108. *See id.*

109. Pub. L. No. 106-102, 113 Stat. 1338.

110. *See* 15 U.S.C.A. § 6802 (West Supp. 2000).

111. *See id.*

112. *See* 15 U.S.C.A. § 6808 (West Supp. 2000).

by the law,[113] bank/insurance company information sharing can take place absent restrictions by other federal or state laws.

The Gramm-Leach-Bliley legislation does not include health information within the definition of protected "nonpublic personal information."[114] The federal functional regulators that were required to issue implementing regulations[115] have not acted to address health information.[116]

The law does, however, contain a provision permitting the customer to "opt-out" of disclosure of nonpublic personal information to third parties.[117] That is, the customer must make affirmative authorization to the company holding the healthcare information that he or she does not want such information disclosed to another party. This concept is contrary to the Department of Health and Human Services health privacy regulations which mandate that a customer "opt-in" before such disclosure can take place.[118] While "opting-out" requires the customer to contact the company, "opting-in" requires that the company contact the customer to get permission before disclosing nonpublic personal information. The FTC has recognized this conflict and commented that compliance with the affirmative authorization provisions of HIPAA would satisfy the opt out requirements under the financial privacy rules.[119]

At this time, there is no broad-based federal statute that applies to patient privacy in general or electronic patient privacy rights in particular.[120] States have enacted most of the laws regarding healthcare privacy. However, a recent survey of these state laws indicates that there are large gaps in the protection provided and enforcement is uneven.[121]

---

113. *See* 15 U.S.C.A. § 6809(6) (West Supp. 2000). An affiliate is defined as "any company that controls, is controlled by, or is under common control with another company." *Id.*

114. 15 U.S.C.A. § 6809(4) (West Supp. 2000).

115. The federal functional regulators are the Office of the Comptroller of the Currency, the Board of Directors of the Federal Deposit Insurance Corporation; the Director of the Office of Thrift Supervision; National Credit Union Administration Board, the Securities and Exchange Commission and the Board of Governors of the Federal Reserve System. *See* 15 U.S.C.A. § 6809(3) (West Supp. 2000).

116. *See* 65 Fed. Reg. 12,354 (2000) (proposed rule of Securities and Exchange Commission on privacy of consumer financial information); 65 Fed. Reg. 10,988 (2000) (proposed rule of National Credit Union Administration on privacy of consumer financial information); 65 Fed. Reg. 8,770 (2000) (joint notice of proposed rule by the Department of the Treasury, Federal Reserve System, Federal Deposit Insurance Corporation on privacy of consumer financial information).

117. *See* 15 U.S.C.A. § 6802(b)(1) (West Supp. 2000). The final regulations promulgated by the Federal Trade Commission provide further detail of this opt out concept. *See* 65 Fed. Reg. 33,646, 33,363-64 (2000).

118. *See id.* at 33,648

119. *See id.*

120. *See* Hodge, *supra* note 44, at 1467-68.

121. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,920 (1999) (to be codified at 45 C.F.R. pts. 160-64) (citing INSTITUTE OF HEALTH CARE

The National Association of Insurance Commissioners (NAIC) promulgated the Health Information Privacy Model Act last year. The purpose of the NAIC Act is to "set standards to protect health information from unauthorized collection, use and disclosure by requring insurance carriers to establish procedures for the treatment of all health information."[122] As of January 2000, five states had passed related legislation or regulation related to the NAIC Act.[123]

VII. PROPOSED REGULATION OF MEDICAL INTEGRATED SYSTEMS

Several bills dealing with encryption have been filed in the 106th Congress. The Security and Freedom through Encryption (SAFE) Act, sponsored by Rep. Bob Goodlatte, a Republican from Virginia, and Rep. Zoe Lofgren, a Democrat from California, would permit use of any kind of encryption in the United States and amend the Export Administration Act of 1979, relating to international sales of encryption software and hardware products.[124] While a house bill sponsored by Representative Porter Goss, a Florida Republican, deals with the same issues as the SAFE Act, it also specifically allows government "backdoor access to the plain text of the encrypted data."[125] Although a court order would be required, the bill essentially mandates that an entity doing business with a government connection (such as a healthcare provider dealing with Medicare or Medicaid) use a means of encryption to which the government would have ultimate access.[126] Privacy advocates have expressed concern over such a requirement.[127] Two other encryption bills are pending in Congress covering the same areas, but neither was slated for immediate consideration.[128]

RESEARCH AND POLICY, THE STATE OF HEALTH PRIVACY: AN UNEVEN TERRAIN (July 1999), *available at* <http://www.healthprivacy.org>).

122. ACCIDENT & HEALTH INS. CONSUMER PROTECTION PRIVACY MODEL ACT § 2 (2000).

123. Telephone Interview with Wendy Pellow, Legislative Counsel for Health Policy, National Association of Insurance Commissioners (July 19, 2000). These states are: Colorado, Delaware, Hawaii, North Dakota, and Wisconsin. *Id.*; *see* COLO. REV. STAT. § 6-18-103 (1999) (privacy of health information collected by cooperatives); DEL. CODE ANN. tit. 16, § 9113 (Supp. 1998) (privacy of health information collected by managed care organizations); HAWAII REV. STAT. §§ 323C-21, 323C-22, 323C-23 (Supp. 1999); N.D. CENT. CODE § 26.1-36-12.4 (Supp. 1999); WISC. STAT. § 610.70 (1998).

124. *See* H.R. 850, 106th Cong. (1999).

125. The Encryption for the National Interest Act of 1999, H.R. 2616, 106th Cong.

126. *See id.* §§ 201, 203 ("The President may require as a condition of any contract by the Government with a private sector vendor that any encryption product used by the vendor in carrying out the provisions of the contract with the Government include features and functions that enable the timely decryption of encrypted data, including communications, or timely access to plaintext, by an authorized party without the knowledge or cooperation of the person using such encryption products or services.").

127. *Summary of Encryption Bills in the 106th Congress*, TECH. L.J. (online journal) <http://www.techlawjournal.com/cong106/encrypt/Default.htm>.

128. *See* Promote Reliable On-Line Transactions to Encourage Commerce and Trade

The goal of the HIPAA mandated Department of Health and Human Services proposed regulation Provisions is to encourage increased and proper use of electronic information while at the same time protecting the needs of patients to safeguard their privacy.[129] However, the Department of Heath and Human Services acknowledged that "the proposed privacy standards would entail substantial initial and ongoing administrative costs for entities subject to the rules"[130]—"this includes the smallest provider to the largest, multi-state health plan."[131]

Under the proposed regulations, no patient authorization is necessary for health plans,[132] healthcare clearinghouses,[133] and healthcare providers[134] ("covered entities") to electronically transmit individually identifiable health information for treatment, payment, and operations.[135] The information could also be disclosed without authorization for specific public policy-related reasons.[136] The covered entities would be mandated to disclose the information only when necessary for compliance with the public policy purposes[137] or when the patient requests inspection and copying.[138] Patient consent is required for any other use or disclosures.[139]

Where no authorization is required, the proposed regulations place restrictions on both internal uses and external disclosures to protect the information.[140] Only the minimum amount of information necessary to

---

(PROTECT) Act, S. 798, 106th Cong. (1999); Electronic Rights for the 2lst Century Act, S. 854, 106th Cong. (1999).

129. *See id.*

130. *Id.* at 59,922.

131. *Id.* at 59,939.

132. A "health plan" is defined as an individual or group plan that provides for, or pays the cost of medical care including employee welfare benefit plans, state regulated insurance plans, managed care plans and all government health plans including Medicare, medicaid, veterans healthcare program and plans operating in the Federal Employee Health Benefits Program. *See* 42 U.S.C. § 1320d(5) (Supp. IV 1998).

133. A "healthcare clearinghouse" is "a public or private entity that processes or facilitates the processing of nonstandard data elements of heath information into standard data elements." 42 U.S.C. § 1320d(2) (Supp. IV 1998).

134. A "healthcare provider" is "a provider of services (as defined in section 1395x(u) of this title), and provider of medical or other health services (as defined in section 1395x(s) of this title), and any other person furnishing healthcare services or supplies." 42 U.S.C. § 1320d(3) (Supp. IV 1998).

135. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,940 (1999) (to be codified at 45 C.F.R. pts. 160-64).

136. *See id.* at 59,955. These "public policy purposes" include: oversight of the public healthcare system, public health functions, research, judicial and administrative proceedings, law enforcement, emergency circumstances, to provide information to next of kin, identification of the body of a deceased person for the cause of death, for government health data systems, for facility patient directories, to banks to process healthcare premiums and payments, and for management of active duty military and other special classes of individuals. *See id.* at 60,056-59.

137. *See id.* at 60,063.

138. *See id.* at 60,059.

139. *See id.* at 60,055. For example, the disclosure of the information to the employer for employment related determinations; the use of information for fund raising purposes; the sale barter or rent of the information or for marketing would require patient authorization. *See id.* at 59,941.

140. *See id.* at 59,924.

accomplish the intended purpose may be disclosed.[141] Individuals can request further use or disclosure for treatment, payment and healthcare operations but the covered entity must agree to the disclosure.[142] The covered entity must ensure that the business partners[143] with whom they share the protected health information are subject to contracts that would limit a business partner's uses and disclosures of protected health information and impose security, inspection, and reporting requirements on the business partner.[144] These standards include a contract that limits the business partner to the uses set forth in the contract and imposes security, inspection, and reporting requirements on the business partner.[145] The regulations set forth explicit requirements which must be in any contract between the covered entity and anyone to whom it gives the protected information.[146]

In order to safeguard the information, covered entities are required to designate a "privacy official," develop a privacy training program for employees, implement safeguards to protect health information from intentional or accidental misuse, provide a system for complaints about privacy practices, and develop sanctions for employees and business partners who violate the regulation.[147] The covered entity must also document its compliance.[148] The Department of Health and Human Services will develop its own complaint system.[149] The regulation does not preempt state laws—thus, some states may have regulations with stronger privacy provisions.[150]

The National Association of Insurance Commissioners (NAIC) is drafting proposed regulations at a state level[151] that substantially follow

---

141. *See id.* at 59,939.

142. *See id.* at 59,945.

143. A business partner is defined as a person to whom the protected health information is disclosed so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. *See id.* at 59,947. This would include lawyers, auditors, consultants, third-party administrators, healthcare clearinghouses, data processing firms, billing firms, and other covered entities. *See id.*

144. *See id.* at 59,925.

145. *See id.* at 59,947.

146. *See id.* at 59,948.

147. *See id.* at 59,988.

148. *See id.* at 59,993-94.

149. *See id.* at 60,002.

150. *See* 42 U.S.C. § 1320d-2 note (Recommendations with Respect to Privacy of Certain Health Information) (Supp. IV 1998).

151. *See Interim GLBA Compliance Regulations-Preliminary Working Draft* (attachment to Memorandum from Kathleen Sebelius, Chair, National Association of Insurance Commissioners to Privacy Issues Working Group and Interested (June 7, 2000)) [hereinafter *Compliance Regulations*] (on file with author). The Federal Trade Commission noted that Section 505 of the G-L-B Act explicitly committed the enforcement jurisdiction over "persons engaged in providing insurance" to state insurance authorities, thus excluding them from the FTC's authority. *See* 65 Fed. Reg. 33,646, 33,648 (2000).

the provisions of the Gramm-Leach-Bliley law for personal non-health information, but which currently reflect the opt-in provision of the Department of Health and Human Services regulations and its own NAIC Health Information Privacy Model Act, for personal health information.[152] However, in addition, the proposed NAIC regulations contain provisions for disclosure of protected health information *without* authorization similar to the provision found in either the NAIC Health Information Privacy Model Act or the Department of Health and Human Services regulation.[153]

Representative James A. Leach, Chairman of the U.S. House of Representatives' Committee on Banking and Financial Services, has proposed specific federal legislation, the Medical Financial Privacy Protection Act,[154] that would prohibit financial institutions from sharing medical financial records and prohibit them from using medical information in making credit decisions. It would also require the customer to opt-*in* before individually identifiable health information could be disclosed to a third party.[155]

VIII. SHORTCOMINGS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES PROPOSED PRIVACY REGULATION PROVISIONS

Unfortunately, while these regulations make important strides in privacy enforcement, they leave many gaps that are fatal to fail-safe privacy protection for patients. For instance, the "covered entities" do not cover all of the entities that may be involved in an integrated system and have access to the same personally identifiable information. As an example, third party administrators, contractors, researchers, workers compensation carriers, life insurance issuers, employers,[156] marketing firms, and outsourced legal, accounting, and administrative services would not be covered by the Department of Health and Human Services' Provisions.[157] Even more disturbing is the total exemption of banks from HIPAA and its subsequent regulations.[158]

---

152. *See Compliance Regulations, supra* note 150, § 19.

153. *See Compliance Regulations, supra* note 150, § 20.

154. H.R. 4585, 106th Cong. (2000).

155. *See* Leach press release, *supra* note 105.

156. The National Committee on Quality Assurance has adopted a standard for the year 2000 that would require health plans to "have policies that prohibit sending identifiable personal health information to fully insured or self-insured employers and provide safeguards against use of information in any action relating to an individual." *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,937 (1999) (to be codified at 45 C.F.R. pts. 160-64) (quoting NATIONAL COMMITTEE FOR QUALITY ASSURANCE 2000 STANDARDS, Standard R.R. 6).

157. *See id.* at 59,924-25.

158. *See* 42 U.S.C. § 1320d-8 (Supp. IV 1998). The Administrative Simplification Provisions are

Moreover, the definition of "transactions" covered under the law is not inclusive of all of the transactions which heath information technology companies now perform and propose to perform in the future.[159] The Department of Health and Human Services' regulations could be improved with a generalized coverage of all aspects of electronic transmissions of personal identifiable healthcare information rather than attempting to be "transaction-specific" in an age where electronic innovation far outpaces government action. Additionally, if the information is on paper, rather than in electronic form, regulations leave medical records unprotected unless and until an electronic version of the Information is made; only then is the paper version protected. If the same data cannot be subject to the law regardless of its form, the "protection" is limited. As a result, the patient cannot be provided the assurances necessary for confidence in electronic data transmission.

Furthermore, the public policy reasons for disclosure seem overly broad. The Department of Health and Human Services' discussion of inclusive definitions of "public health activities"[160] and "oversight activities"[161] is troublesome in light of the Department of Health and Human Services' acknowledged absence of jurisdiction to prohibit further use and disclosure of the protected information acquired for such activities.[162] This is especially of concern since under the Department of Health and Human Services indicates the "public health," and "oversight activities" can be performed not only by governmental, but also by private entities.[163] While on one hand the government "giveth" patients privacy through healthcare entities, the government "taketh" that same privacy away in terms of public policy use of that same information. The comments to the Department of Health and Human Services proposed privacy regulations provide little comfort that the federal government will not be the biggest offender in the use of personally identifiable information.[164] The enunciated public policy exceptions should be narrowed considerably before final adoption of these regulations.

---

inapplicable to financial institutions or anyone acting on behalf of a financial institution when "authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for a financial institution." *Id.*

159. *See* 42 U.S.C. § 1320d-2(a)(2) (Supp. IV 1998).

160. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,956 (1999) (to be codified at 45 C.F.R. pts. 160-64).

161. *See id.* at 59,957-58.

162. *See id.* at 59,955.

163. *See id.* at 59,956 (explaining that the proposed rule would allow disclosure to non-governmental entities carrying out public health activities); *id.* at 59,958.

164. *See, e.g., id.* at 59,925 (Permissible Uses and Disclosures for Purposes Other Than Treatment); *id.* at 59,955 (Uses and Disclosures Permitted Without Authorization).

Lastly, the regulations do not create a private cause of action for the patient.[165] However, recovery under other privacy laws may still be a possibility. If the patient is to be protected, then the patient should be entitled to redress if the law is not followed. Criminal penalties appear to be excessive in such a situation, especially at a time when the Internet is a burgeoning and developing experiment. The monetary penalties may serve as a deterrent to disclosure but provide little solace to the individual who must bear the brunt of the consequences of such a disclosure. It would be preferable to place a monetary cap on a private civil cause of action concurrent with state and federal jurisdiction than to create another level of governmental bureaucracy for enforcement of this regulation.

Federal privacy legislation or privacy regulations should track or follow that portion of California's Personal Information and Privacy Act of 1999 as originally introduced. California's Personal Information and Privacy Act would require organizations to inform individuals about the type of information it collects, how it collects the information, the types of organizations to whom it is disclosed, and the means the organization uses to limit the use and disclosure of the information.[166] Under such a law, the patient would know in advance the extent of disclosure anticipated and could make informed choices.

IX. LIABILITY EXPOSURE FOR HEALTHCARE PROVIDERS

Healthcare providers who do not conduct the electronic transactions themselves would become subject to the policies if another entity, such as a billing agent or hospital, transmits health information on their behalf.[167] If a company providing healthcare information systems is denominated the source of the transmission, vicarious liability would, in all probability, inure to the provider of the integrated system. A healthcare provider should seek an indemnification agreement to protect itself. In addition, a company providing healthcare information systems could very well be deemed to be a "business partner" with whom the healthcare providers are sharing the protected information. In such case, healthcare providers must draft contract language with any entity providing healthcare information systems to provide specific limitations on disclosure of identifiable health information and impose security,

165. *See id.* at 59,923.

166. *See* S. 129, 1999-2000 Leg., 1st Sess. (Cal. 1999); *see also* Internet Growth and Development Act of 1999, H.R. 1685, 106th Cong. § 301 (requiring operator of a commercial website to provide notice of its policy regarding use of personal information, including disclosure to third parties).

167. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,925 (1999) (to be codified at 45 C.F.R. pts. 160-64).

on disclosure of identifiable health information and impose security, inspection and reporting requirements for the electronic software providers. In addition, a healthcare provider, small or large, should have in place a privacy policy appropriate to its size, information practices and its business requirements.[168] Then, if and when the government would investigate any alleged breach, it can legitimately be argued the deviation was a breach of that existing policy.

X. ENTITIES OF THE FUTURE

The future of companies providing healthcare information systems seem positive from an economic perspective. These companies are projected to increase healthcare efficiency and decrease healthcare costs. These companies also seek to bring all of the discrete parts and functions of the healthcare system together in one seamless web. However, this gain must more than offset the cost of compliance with privacy laws.

This bright future may be dimmed when the dynamic legal developments in the area of privacy protection are considered. While many regulations have not been adopted and remain subject to change as a result of public comment or political winds, there is a definite movement to tighten control over healthcare information systems. Congress may still prevent the regulations from being adopted by taking action pursuant to its own mandate in HIPAA. Encryption legislation may be pushed to a vote before the 106th Congress ends. Courts may extend the "right to privacy" to a new level. States may adopt the National Association of Insurance Commissioners Model Act regarding healthcare privacy, or other state legislation. The effect any new regulations will have on healthcare information companies is unknown. The companies, the innovations, and the application of the law of privacy to this new virtual reality bear close watching as the new millennium continues.

---

168. *See id.*

* * *