Journal of Health Care Law and Policy

Volume 12 | Issue 1 Article 4

Privacy and Confidentiality in the Age of E-Medicine

Keith A. Bauer

PRIVACY AND CONFIDENTIALITY IN THE AGE OF E-MEDICINE

KEITH A. BAUER, MSW, PH.D.

INTRODUCTION

What is today commonly referred to as *e-medicine*[1] is increasingly employed to provide medical services to patients (clinical applications)[2] and to manage, store, and transmit patient health information (non-clinical or administrative applications).[3] Commonplace information and communication technologies used in e-medicine include (a) electronic health records (EHR), (b) electronic mail (e-mail), (c) digital video recordings, and (d) online or Internet-based networks that link insurance companies, hospitals, individual healthcare professionals, and patients.[4] E-medicine has a number of already proven benefits, including improvements in health care quality; prevention of medical errors; reduced health care costs; increased administrative efficiencies; decreased paperwork, and expanded access to healthcare.[5]

The growth of e-medicine, however, has also exacerbated the threat of privacy intrusions, with potentially deleterious results for health care quality, provider-patient relationships, and patients' overall confidence in our health care system.[6] There are a number of specific means by which personal health

---

1. *See* John H. Stone, *Communication Between Physicians and Patients in the Era of E-Medicine*, 356 NEW ENG. J. MED. 2451, 2451–53 (2007) (describing different models of *e-medicine* and the objective of certain types). Other neologisms include *cybermedicine, e-health, telemedicine, and telehealth*. *See* Meghan Hamilton-Piercy, Note, *Cybersurgery: Why the United States Should Embrace This Emerging Technology*, 7 J. HIGH TECH. L. 203, 205–06 & n.11 (2007).

2. *See* James C. Martin et al., *The Future of Family Medicine: A Collaborative Project of the Family Medicine Community*, ANNALS FAM. MED., Mar.–Apr. 2004, at S3, S13; Sarah E. Born, Note, *Telemedicine in Massachusetts: A Better Way to Regulate*, 42 NEW ENG. L. REV. 195, 200–01 (2007). Two of the most common clinical applications are teledermatology and telepsychiatry. Born, *supra*, at 200–01.

3. *See* Edward Fotsch, *E-Medicine in the Physician's Office*, *in* MEDICAL MALPRACTICE: A PHYSICIAN'S SOURCEBOOK 75, 75, 83–87 (Richard E. Anderson ed., 2005); Martin et al., *supra* note 2, at S13; Stone, *supra* note 1, at 2451–52.

4. Fotsch, *supra* note 3, at 75, 80–81; Stone, *supra* note 1, at 2451–53; Born, *supra* note 2, at 200–01.

5. U.S. Dep't of Health & Human Servs., Health Information Technology, http://healthit.hhs.gov/portal/server.pt (last visited Sept. 23, 2009).

6. Keith Bauer, *Cybermedicine and the Moral Integrity of the Physician-Patient Relationship*, 6 ETHICS & INFO. TECH. 83, 89 (2004).

information (PHI) can be compromised. First, there is the threat of cookies and spyware, which allow unauthorized persons to monitor computer use and track online activities, such as the websites patients visit.[7] Second, there is the threat that hackers will gain illicit access to patient records simply because they can, or for more nefarious ends such identity theft.[8] Third, patient information may be transmitted to unauthorized persons accidentally or even the World Wide Web.[9] Fourth, and probably the greatest threat to privacy, involves the human element—in particular, poorly designed security measures and the inadequate training of staff.[10] Lastly, there are multiple privacy standards and incompatible security measures among entities that have access to patient information, making it more likely that patients' health-related information will fall into the wrong hands.[11]

I. DEFINING PRIVACY

What exactly are we talking about when we discuss privacy, and why is it so important for the practice of effective and ethical medicine? In answering these questions, we can look to one of the earliest statements on medical privacy, the Hippocratic Oath. According to the ancient oath taken by fledgling physicians:

> What I may see or hear in the course of the treatment or even outside of treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about.[12]

One thing to note about the Oath is that the emphasis is entirely on the physician's duty to maintain patient privacy. The Oath makes no reference to patient autonomy or physician-patient collaboration. This is because the Hippocratic tradition is highly paternalistic. Patients are passive recipients of physician expertise; of what the physician deems to be in the best interest of his patients. Unlike the Hippocratic view, contemporary views on medical privacy

7. *See* Fotsch, *supra* note 3, at 82–85; George Lawton, *Invasive Software: Who's Inside Your Computer?*, COMPUTER, July 2002, at 15, 15–16; Sonia W. Nath, Note, *Relief for the E-patient? Legislative and Judicial Remedies to Fill HIPAA's Privacy Gaps*, 74 GEO. WASH. L. REV. 529, 534–36 (2006).

8. *See* Randolph C. Barrows & Paul D. Clayton, *Privacy, Confidentiality, and Electronic Medical Records*, 3 J. AM. MED. INFORMATICS ASS'N 139, 140 (1996).

9. *See, e.g.*, Jeff Collmann & Ted Cooper, *Breaching the Security of the Kaiser Permanente Internet Patient Portal: The Organizational Foundations of Information Security*, 14 J. AM. MED. INFORMATICS ASS'N 239, 239 (2007).

10. *See* Fotsch, *supra* note 3, at 83–84 (describing suggested guidelines for *e-medicine* security).

11. *See* Sharona Hoffman & Andy Podgurski, *Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 HARV. J.L. & TECH. 103, 132–34 (2008) (explaining the current problems with industry-run regulation of electronic health records in the United States).

12. LUDWIG EDELSTEIN, ANCIENT MEDICINE 6 (Owsei Temkin & C. Lilian Temkin eds., Johns Hopkins Univ. Press 1987).

place significant emphasis on patients, especially their autonomy and ability to maintain some control over PHI.[13]

The now-classic definition of privacy was articulated by Alan Westin, who argued that "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[14] Westin's definition of medical privacy improves on the Hippocratic Oath and is in line with our democratic sensibilities, but does not encompass all types of privacy. In the context of e-medicine, discussions of privacy tend to focus on *informational privacy*. But e-medicine also has implications for *physical privacy* as well.[15] To illustrate this distinction, consider telemedicine patients who remotely receive health care. Telemedicine patients can achieve greater physical privacy by reducing the number of home care visits, but put at risk the informational privacy of their medical data as it streams over the Internet, standard telephone lines, and various wireless technologies. What should be noted about this example is that not only are there at least two kinds of privacy, but that these two kinds of privacy can come into conflict with each other, potentially requiring tradeoffs between them.[16]

A. Privacy & Confidentiality

To understand better the complex nature of privacy, it is also necessary to recognize the similarities and differences between privacy and confidentiality. Both privacy and confidentiality generally refer to limiting access to one's body, thoughts, feelings, documents, and living spaces.[17] Also, both concepts refer to information that is out of the public domain.[18]

---

13. *See* James G. Hodge, Jr. & Kieran G. Gostin, *Challenging Themes in American Health Information Privacy and the Public's Health: Historical and Modern Assessments*, 32 J.L. MED. & ETHICS 670, 671 (2004) (noting that the modern focus on respect for individual autonomy has influenced the foundations of health information privacy protections).

14. ALAN F. WESTON, PRIVACY AND FREEDOM 7 (1967).

15. Keith A. Bauer, *Home-Based Telemedicine: A Survey of Ethical Issues*, 10 CAMBRIDGE Q. HEALTHCARE ETHICS 137, 139–40, 143 (2001). *See generally* RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 15–16, 35–36 (1989) (explaining the concept of *physical privacy* in general).

16. Bauer, *supra* note 15, at 143.

17. *Compare* WACKS, *supra* note 15, at 15–16 (describing the features of privacy as limited accessibility to information, physical contact, and identity of the individual), *with* DEAN M. HARRIS, HEALTHCARE LAW AND ETHICS ISSUES FOR THE AGE OF MANAGED CARE, 176 (1999) (describing the duty of confidentiality as the duty to refrain from disclosing and prevent others from disclosing personal information).

18. *See* 1 PRIVACY, at xi (Raymond Wacks ed., 1993) (describing the broad concept of privacy as predicated upon the differentiation between public and private spheres); WACKS, *supra* note 15, at 51–53 (noting that an action for breach of confidentiality will not lie when the information in question is in the public domain).

There are, however, important differences between confidentiality and privacy. First, confidentiality consists of a complex set of moral, social, and legal practices that work to protect one's privacy.[19] Second, confidentiality requires at least one person to give up his privacy to another person in the context of a trust-based relationship.[20] In health care settings, confidentiality requires that patients disclose health-related information to their health care providers, who in turn promise to maintain confidence.[21] Disclosure can take the form of a verbal medical history or a physical examination. In both cases, patients reveal themselves for the purpose of obtaining medical treatment. Thus, unlike privacy, confidentiality is always relational and must include at least two persons or agents, one of whom discloses private information to another with the expectation that the disclosed information will remain confidential.[22]

If the privacy and confidentiality of patient information cannot be secured, patients will be less likely to trust their health care providers and less likely to share personal information, particularly stigmatizing information such as risky sexual activity, chemical abuse, and mental health problems. Fear of disclosing sensitive information would make it even more difficult for health care providers to obtain adequate patient histories, make correct diagnoses, and provide patients with appropriate treatments. In short, without privacy and confidentiality protections, health care providers will be unable to do their jobs effectively.

The importance of privacy and confidentiality is obvious, but what are the normative grounds for privacy and confidentiality? That is, what are the ethical values and principles that justify privacy and confidentiality?

II. ETHICAL JUSTIFICATIONS FOR CONFIDENTIALITY AND PRIVACY

A. Consequentialist Justification

From a consequentialist perspective, privacy and confidentiality have *instrumental value* because they serve to promote important social goals, including the enhancement of individuality, self-determination, and the freedom to cultivate intimate relationships free from public life.[23] Without a clear demarcation between

19. Benedict Stanberry, *Legal and Ethical Aspects of Telemedicine*, 12 J. TELEMEDICINE & TELECARE 166, 167–168 (2006).

20. *See* HARRIS, *supra* note 17, at 176 (noting that physicians must obtain confidential and sometimes embarrassing information from patients to provide appropriate care, and that patients must trust providers when providing candid information).

21. *Id.*

22. *See* LeRoy Walters, *Ethical Aspects of Medical Confidentiality*, *in* CONTEMPORARY ISSUES IN BIOETHICS 198, 199–200 (Tom L. Beauchamp & LeRoy Walters eds., Wadsworth Publ'g Co. 2d ed. 1982) (1978) (distinguishing privacy's focus on sheltering an individual's own secrets from the duty of confidentiality, in which the distressed patient shares private information with the physician and thereby "admits the physician to an inner circle" of private information and creates the physician's duty).

23. *See* James Rachels, *Why Privacy is Important*, 4 PHIL. & PUB. AFF. 323, 326 (1975).

public and private domains, autonomous individuals and voluntary relationships would be difficult, if not impossible, to achieve.[24]

In the health care realm, a consequentialist justification of privacy and confidentiality has ethical significance because it addresses specific goals such as the promotion of provider-patient relationships and the protection of patients' social status. More generally, privacy and confidentiality have instrumental value because they can help to maximize good patient care and minimize potential patient harm. These two ends are encapsulated in the ethical principles of *beneficence* (i.e., promote the medical good of patients) and *non-malfeasance*, or *primum non nocere* ("first of all, do no harm" to patients).[25] Health care institutions and individual providers who fail to protect patient privacy and confidentiality violate these fundamental principles.

B. Deontological Justification

Unlike a consequentialist approach, a deontological approach (i.e., rule- or duty-based ethics) does not ethically justify privacy and confidentiality by their utility.[26] Instead, deontological justifications justify privacy and confidentiality in terms of *respect for persons*, which is grounded in the fundamental principle of *autonomy*.[27] From a deontological standpoint, privacy and confidentiality are justified in terms of the *intrinsic value* and dignity of autonomous persons, not their instrumental value and the ends they serve.[28] Stated differently, privacy and confidentiality help to protect the moral agency of patients by allowing them to live their lives as they choose.[29] In light of these deontological considerations, many countries and international treaties consider privacy to be a fundamental and unalienable right. For example, both the UN Declaration of Human Rights and the International Covenant on Civil and Political Rights recognize the right to privacy.[30] In these treaties, privacy is recognized as a form of autonomy—a way to ensure protection from "arbitrary interference."[31]

---

24. Rem B. Edwards, *Confidentiality and the Professions*, *in* BIOETHICS 72, 76–78 (Rem B. Edwards & Glenn C. Grader eds. 1988).

25. Raanan Gillon, *Medical Ethics: Four Principles Plus Attention to Scope*, 309 BRIT. MED. J. 184, 185 (1994) (defining beneficence and non-malfeasance).

26. *See* Gerald F. Gaus, *What is Deontology? Part One: Orthodox Views*, 35 J. VALUE INQUIRY 27, 28 (2001). This does not mean consequences have no significance for deontological justifications; it means only that consequences have a secondary role. *Id.*

27. *See id.*; Barbara Secker, *The Appearance of Kant's Deontology in Contemporary Kantianism: Concepts of Patient Autonomy in Bioethics*, 24 J. MED. & PHIL. 43, 47, 56 (1999).

28. *See* Secker, *supra* note 27, at 47, 56.

29. *See* WESTON, *supra* note 14, at 7.

30. Universal Declaration of Human Rights, G.A. Res. 217A, at 71, 73–74, U.N. GAOR, 3d Sess., 183d plen. mtg., U.N. Doc A/810 (Dec. 10, 1948); International Covenant on Civil and Political Rights, G.A. Res. 2200A, at 49, 55, U.N. GAOR, 11th Sess., 1496th plen. mtg., U.N. Doc. A/6316 (Dec. 16, 1966).

31. Universal Declaration on Human Rights, *supra* note 30, at 73–74.

III. PUBLIC CONCERNS

A 2000 survey of Internet users found that 75 percent of respondents were worried that health sites shared information without consent and that a full 17 percent would not even seek health information on the web due to privacy concerns.[32] The same poll also found that 61 percent of Americans felt that too many people have access to their medical records.[33] Little has changed since that poll was conducted. In July 2008, for example, a Harris poll concluded that millions of Americans believe medical records have been compromised.[34] Is this simply an irrational fear unsubstantiated by evidence? The short answer is no. There are numerous cases in which identifiable patient health information has been compromised.

A. Case 1

In February 2008, a researcher's laptop computer was stolen.[35] The laptop contained the health data of 2,500 subjects who were participating in a medical trial conducted by the National Institutes of Health (NIH).[36] Prior to our ability to store health information on laptops in a digital format, it would have been virtually impossible for someone to steal, at one time, the health data of 2,500 patients. Moreover, unlike traditional paper record keeping, digitally stored data is easily replicated and transmitted on the World Wide Web, from where it can be downloaded to a limitless number of personal computers. It should be noted that this case is a not a matter of failed technology; rather, it is a clear example of human error and neglect.

B. Case 2

In a second case involving the NIH, the DNA profiles of 60,000 patients were removed from a public database because a study revealed that a new type of analysis could be used to confirm identities and that patients' genetic information was not as anonymous as first thought.[37]

---

32. Janlori Goldman & Zoe Hudson, *Virtually Exposed: Privacy and E-Health*, HEALTH AFF., Nov.–Dec. 2000, at 140, 141 (2000).

33. Jedediah Purdy, *An Intimate Invasion*, USAWEEKEND.COM, July 2, 2000, http://www.usaweekend.com/00_issues/000702/000702privacy.html.

34. Harris Interactive, Millions Believe Personal Medical Information Has Been Lost or Stolen: Issue a Roadblock to Acceptance of Electronic Health Record Systems (July 15, 2008), *available at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=930.

35. Editorial, *Safeguarding Private Medical Data*, N.Y. TIMES, Mar. 26, 2008, at A22.

36. *Id.*

37. Jason Felch, *DNA Profiles Blocked from Public Access*, L.A. TIMES, Aug. 29, 2008, at A31. *See generally* Sheri A. Alpert, *Protecting Medical Privacy: Challenges in the Age of Genetic Information*, 59 J. SOC. ISSUES 301 (2003) (discussing genetic privacy).

C. *Case 3*

Telemetry-capable medical devices also pose a threat to medical privacy. In one case, researchers found that implantable cardiac defibrillators and pacemakers equipped with wireless technology, which permit remote device checks and the transmission of a patient's vital signs, can be hacked, allowing unauthorized individuals to gain access to an individual's PHI.[38] Equally disturbing is that once security has been breached, a hacker can reprogram a device without the knowledge and consent of the patient.[39]

D. *Case 4*

In a highly publicized case in 2000, Kaiser Permanente (KP) employees accidentally mailed 800 patients' personally identifiable health information (e.g. appointment details, answers to patients' questions, medical advice) to other patients and employees within the KP network.[40] According to KP, the breach occurred at KP's web-enabled health care portal and was the result of systemic problems within the KP organization.[41] The systemic problems included the architecture of the information system, the motivations of individual staff members, differences among the subcultures of individual groups within the organization, as well as technical and social relations across the KP's IT program.[42]

With the above cases in mind, it is not surprising that many patients and health care professionals alike are skeptical of e-medicine and the threat it posses to medical privacy.

IV. MISUSES OF PATIENT HEALTH DATA

Threats to the privacy and confidentiality of personal health data are not new. The rise of e-medicine broadened the scope and magnitude of the threats. Digitalization made it easier for authorized and unauthorized persons to collect, store, replicate, and transmit acquired patient data. Once PHI is collected, legally or illegally, there are a number of ways in which this information can be misused.

First, patient health-related information could be commercially misused. In recent years, an extensive data market has developed, driven largely by data aggregators, who repackage and sell information without the knowledge or consent

38. Daniel Halperin et al., *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*, *in* 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 129, 129–30, 133–35, *available at* http://www.secure-medicine.org/icd-study/icd-study.pdf.

39. *Id.* at 136–37.

40. Collmann & Cooper, *supra* note 9 *passim*; Bill Brubaker, *'Sensitive' Kaiser E-Mails Go Astray*, WASH. POST, Aug.10, 2000, at E1.

41. Collmann & Cooper, *supra* note 9 *passim*; Brubaker, *supra* note 40, at E1.

42. Collmann & Cooper, *supra* note 9, at 242–43.

of the original information owner.[43] Commercial misuses of data can have several serious consequences for individuals, leading, for example, to a denial of insurance coverage or credit, or to invasive unsolicited marketing programs.[44]

Second, criminals can misuse patient health-related information. Identity theft represents a particularly serious problem. In 2003, the FTC estimated that ten million Americans (nearly 5 percent of the adult population) were victims of some form of identity theft.[45] According to the FBI, the Internet Crime Complaint Center received more than 20,000 complaints regarding identity theft in the five-year period between its opening in 2000 and 2005.[46]

The third and most serious threat comes from our own government. According to a 2004 report issued by the Government Accountability Office (GAO), fifty-two federal agencies and departments reported 199 data mining efforts, of which sixty-eight were planned and 131 were operational.[47] The most common reasons cited by the GAO for data mining included improvements in service or performance; detection of fraud, waste, and abuse; analysis of scientific and research information; management of human resources; detection of criminal activities or patterns; and analysis of intelligence and detecting terrorist activities.[48]

The GAO report identified the Department of Defense as having the largest number of data mining efforts aimed at analyzing intelligence and detecting terrorist activities, followed by the Departments of Homeland Security, Justice, and Education. The Department of Education reported the largest number of efforts aimed at detecting fraud, waste, and abuse. Data mining efforts for detecting criminal activities or patterns, however, were spread relatively evenly among the reporting agencies.[49]

In addition, out of all 199 data mining efforts identified, 122 used personal information.[50] For these efforts, the primary purposes were detecting fraud, waste, and abuse; detecting criminal activities or patterns; analyzing intelligence and

43. Nicole Duarte, *Consumer Protections Are Few in the Growing Data Broker Industry*, MARKET WATCH, Sept. 8, 2006.

44. *Id.*; Electronic Privacy Information Center, SPAM—Unsolicited Commercial E-Mail, http://epic.org/privacy/junk_mail/spam/ (last visited Sept. 23, 2009).

45. FED. TRADE COMM'N, IDENTITY THEFT SURVEY REPORT 13 (2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

46. *See* INTERNET CRIME COMPLAINT CTR., 2007 INTERNET CRIME REPORT 2 chart 1, 5 chart 5, *available at* http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf.

47. U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDER RANGE OF USES 7 (2004), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-04-548. The General Accounting Office was redesignated as the Governmental Accountability Office in 2004. GAO Human Capital Reform Act of 2004, Pub. L. No. 108-271, §§ 1(a), 8(a), 118 Stat. 811, 811, 814 (2004).

48. U.S. GEN. ACCOUNTING OFFICE, *supra* note 47, at 7.

49. *Id.* at 7–8.

50. *Id.* at 10.

detecting terrorist activities; and increasing tax compliance.[51] Personal information collected from other federal agencies and the private sector included credit reports, credit card numbers and transactions, student loan application data, bank account numbers, and taxpayer identification numbers.[52] Movement toward a nationwide health records system will provide additional opportunities for government to more easily mine, aggregate, and misuse PHI if it should elect to do so.[53]

V. FAIR INFORMATION PRACTICES

In 1980, the Organization for Economic Cooperation and Development (OECD) released eight guidelines to protect individual privacy while facilitating the free flow of personal data between countries in the conduct of commerce.[54] The United States approved the eight OECD guidelines, which are also known as "fair information practices" (FIPs), and incorporated them into subsequent privacy regulations promulgated by the Department of Health and Human Services (HHS) in 2003[55] under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[56] The eight guidelines address collection limitation, data quality, specification of purpose, use limitation, security safeguards, openness regarding data policies and procedures, individual participation, and accountability.[57]

One thing the FIPs do well is specify the entities covered by them, including defining "protected health information."[58] Essentially, PHI is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium, excluding some classes of records such as mental health records.[59] The regulations define "covered entities" as health plans, health clearinghouses, health care providers, and business associates who transmit health information in an electronic format.[60]

---

51. *Id.* at 7–12.

52. *Id.* at 10–11.

53. *See infra* Parts VI–VII.

54. ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://it.ojp.gov/documents/OECD_FIPs.pdf.

55. U.S. DEP'T OF HEALTH & HUMAN SERVS., NATIONWIDE PRIVACY AND SECURITY FRAMEWORK FOR ELECTRONIC EXCHANGE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION 2 (2008), *available at* http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_848088_0_0_18/NationwidePS_Framework-5.pdf (describing the influence of the Code of Fair Information Practice on "U.S. laws at both the Federal and state levels").

56. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, and 42 U.S.C.).

57. ORG. FOR ECON. CO-OPERATION & DEV., *supra* note 54, at 14–16.

58. *See* 45 C.F.R. § 164.103 (2008).

59. *Id.*

60. 45 C.F.R. § 164.104 (2008).

In their inception, the intent was to provide a set of FIPs to govern how PHI would be used.[61] The problem, however, with the HIPAA privacy regulations is that the consent requirements did very little to enhance patient autonomy and protect patient privacy. First, although individuals will be notified that their information will be disclosed,[62] they do not get to decide whether or not they want their PHI disclosed.[63] There is an important difference between notification and consent. Second, individuals have the right to request further protections, but their doctors and others do not have to agree to individuals' requests.[64] Third, individuals do not have an absolute right to get copies of their medical records.[65] Clinicians may refuse to share records in some circumstances.[66] Fourth, individuals may request amendments to their medical records, but clinicians are not required to accept a patient's suggested amendments.[67] Furthermore, the privacy rule permits clinicians, hospitals, health plans and other "covered entities" to distribute identifiable patient information without patient consent for so-called "national priority activities."[68]

According to the Institute for Health Freedom, the uses and disclosures for which an authorization is not required include uses and disclosures required by law; uses and disclosures for public health activities; disclosures about victims of abuse, neglect or domestic violence; uses and disclosures for health oversight activities; disclosures for judicial and administrative proceedings; disclosures for law enforcement purposes; uses and disclosures about decedents; uses and disclosures for cadaveric organ, eye or tissue donation purposes; uses and disclosures for research purposes; uses and disclosures to avert a serious threat to health or safety; uses and disclosures for specialized government functions; and disclosures for workers' compensation.[69] As critics have claimed, instead of protecting patient privacy, HIPAA and associated privacy rules have more or less eliminated patient autonomy and consent from the practice of medicine.[70]

---

61. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000).

62. 45 C.F.R. § 164.520(a) (2008) (establishing the individual right to adequate notices of uses and disclosures of PHI).

63. *Id.* § 164.512 (outlining uses and disclosures of PHI for which patient authorization is not required).

64. *Id.* § 164.522.

65. *See id.* § 164.524 (describing right of access to an individual's own protected health information and exceptions to the right).

66. *Id.*

67. *Id.* §164.526.

68. *See id.* § 164.512; OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 6–7 (2003).

69. 45 C.F.R § 164.512(d)–(l).

70. *See, e.g.*, Fred H. Cate, *Principles for Protecting Privacy*, 22 CATO J. 33, 46–50 (2002).

VI. EVOLUTION OF A NATIONAL HEALTH INFORMATION NETWORK

The *Administrative Simplification* portion of HIPPA sought to facilitate greater interoperability among disparate health information systems and sharing of electronic medical data, moving the nation toward a National Health Information Network (NHIN).[71] To create a successful NHIN, the federal government must create:

- Unique Patient IDs (UPI) - a national medical ID card for every citizen;
- National Provider IDs (NPI) - a unique identification number for every doctor, nurse, therapist, hospital, health care facility, and other providers;
- Employer ID Numbers (EIN) - a unique number for every employer;
- A Payer ID - an identification number for every insurer and health plan;
- National codes for all health care procedures;
- National transaction sets; and
- National security standards for health information.[72]

Subsequently, as a way to expedite the creation of the NHIN, President Bush issued Executive Order 13335 on April 27, 2004, establishing the position of a National Coordinator for Health Information Technology (ONC) within the Office of the Secretary of Health and Human Services.[73] The Executive Order mandated that the ONC provide leadership for the development and nationwide implementation of an interoperable health information technology infrastructure by 2014, bringing together all federal activities in health information technology in a coordinated fashion.[74] The strategic plan of the ONC is to improve the quality,

71. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 262(a), 110 Stat. 1936, 2025; *see also* HIPAA Administrative Simplification, 73 Fed. Reg. 49,796, 49,797, 49,808, 49,826 (Aug. 22, 2008); Michael D. Greenberg & M. Susan Ridgely, *Patient Identifiers and the National Health Information Network: Debunking a False Front in the Privacy Wars*, 4 J. HEALTH & BIOMED. L. 31, 31–32, 40–43 (2008).

72. Health Insurance Portability and Accountability Act of 1996, § 262(a), 110 Stat. at 2025.

73. Exec. Order No. 13,335, 3 C.F.R. 160 (2005).

74. *Id.* Although the Executive Order does not state a year, President Bush clearly expressed that 2014 was the target date for an NHIN. Safe Harbors for Certain Electronic Prescribing and Electronic Health Records Arrangements Under the Anti-Kickback Statute, 71 Fed. Reg. 45,110, 45,133 (Aug. 8, 2006) (to be codified at 42 C.F.R. pt. 1001). It should be noted that there are a number of state initiatives working along side the federal government to achieve a NHIN. *See, e.g.*, NAT'L GOVERNORS ASS'N, THE STATE ALLIANCE FOR E-HEALTH, ACCELERATING PROGRESS: USING HEALTH INFORMATION TECHNOLOGY AND ELECTRONIC HEALTH INFORMATION EXCHANGE TO IMPROVE CARE (2008), *available at* http://www.nga.org/Files/pdf/0809EHEALTHREPORT.PDF; Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y L. & ETHICS 327, 338–39 (2002). In addition to the federal government and the states, various medical organizations are also involved in making the NHIN a reality. For example, the American Medical Association (AMA) proposed guidelines to regulate online medical and health information

efficiency and privacy of health-related information, and make health information available to patients for non-medical purposes, as directed by the patient.[75]

As a way of reaching these objectives, the ONC recognized that interoperability not only requires a seamless, integrated network of information technology and unique IDs; but also the establishment of an unambiguous NHIN lexicon.[76] Consequently, ONC contracted The Alliance for Health Information Technology (AHIT) to develop a common NHIN language by reaching consensus on definitions for the following terms: electronic medical record (EMR), electronic health record (EHR), patient health record (PHR), health information exchange (HIE), regional health information organization (RHIO), and health information oversight (HIO).[77]

According to the report issued by AHIT, the term "HIE" is frequently used to describe both the processes of health information exchange and the organizations managing the exchanges.[78] As result, HIEs and RHIOs tend to be used synonymously.[79] To establish greater clarity, the AHIT redefined "HIE" as the process of exchanging information and created a new term, "HIO," to refer to the organizations governing the exchange of information.[80] Under the new definitions, a RHIO is a type of HIO.[81]

Under the new definitions, the primary difference between an EMR and an EHR is the ability to exchange information interoperably.[82] An EMR does not exchange information interoperably, whereas an EHR does.[83] The trend, however, is toward electronic records that are capable of using nationally recognized interoperability standards, which is a key feature of EHRs.[84] By the year 2014, it is anticipated that electronic records not capable of exchanging information

---

websites that would govern (a) content, (b) advertising and sponsorship, (c) e-commerce, and (d) privacy and confidentiality. The AMA also launched Medem, a website that offers health information and allows patients to correspond safely with doctors online and permits secure electronic transactions. According to the Medem website, they expect to provide connectivity between community and regional stakeholders in healthcare, which will fulfill the vision of interoperable health records for all Americans by 2014. Medem, About Medem, http://www.medfusion.net/ihealth/ (last visited Sept. 23, 2009).

75. Exec. Order No. 13,335, 3 C.F.R. § 160 (2005).

76. NAT'L ALLIANCE FOR HEALTH INFO. TECH., DEFINING KEY HEALTH INFORMATION TECHNOLOGY TERMS 8, 21 (2008), *available at* http://www.nahit.org/images/pdfs/HITTermsFinalReport_051508.pdf.

77. *Id.* at 16–26.

78. *Id.* at 5.

79. *Id.*

80. *Id.* at 21–24.

81. *Id.* at 25.

82. *Id.* at 14.

83. *Id.*

84. *Id.*

interoperably will lose their relevance, and the term "EMR" will become obsolete.[85]

Finally, the control of one's health-related information distinguishes the EHR from the PHR.[86] The information in a PHR, whether derived from an EHR or other sources, is for the patient to manage and use.[87] But, when a patient is granted access to his electronic record maintained and controlled by a provider or payer organization, he is accessing an EHR, not his PHR.[88]

VII. PROTECTING MEDICAL PRIVACY AND CONFIDENTIALITY

As discussed earlier, HIPAA privacy rules have at least three significant shortcomings: (1) patient consent and authorization for the use and disclosure of PHI is almost nonexistent; (2) the number of entities that may be included in the class of "covered entities" is legion; and (3) some non-covered entities that receive PHI by covered entities are not required to protect the information once it has been received. As an illustration of these shortcomings, the Department of Labor and the U.S. Census Bureau, relying on data from 2000 and 2004, calculated that close to 15 million people, as employees of covered entities, could be in a position to access and use PHI.[89]

The fact that millions of people might be authorized to access and potentially disclose PHI should make us worry. We should, however, be even more worried, given that the establishment of a NHIN by 2014 could permit even more individuals to access PHI and exacerbate the already limited consent, use, and disclosure requirements operative under HIPAA. If nothing is done, patient privacy and confidentiality, the ethical cornerstone of medicine, could be an unattainable ideal by 2014.[90]

In order to circumvent the flaws of HIPAA's "protections," as well as meet the potential challenges of a NHIN, it is necessary to retool the existing guidelines that regulate the privacy and confidentiality of PHI. The following seven principles are derived from existing laws, statutes, and fair information practices (FIPS).

---

85. *See* Karen M. Bell, *Foreword* to NAT'L ALLIANCE FOR HEALTH INFO. TECH., *supra* note 76, at 3.

86. NAT'L ALLIANCE FOR HEALTH INFO. TECH., *supra* note 76, at 18.

87. *Id.* at 19.

88. *Id.* at 18.

89. Sheri Alpert, *Privacy Issues in Clinical Genomic Medicine, or Marcus Welby, M.D., Meets the $1000 Genome*, 17 CAMBRIDGE Q. HEALTHCARE ETHICS 373, 380 & tbl.1 (2008).

90. *See* Safe Harbors for Certain Electronic Prescribing and Electronic Health Records Arrangements Under the Anti-Kickback Statute, 71 Fed. Reg. 45,110, 45,133 (Aug. 8, 2006) (to be codified at 42 C.F.R. pt. 1001). *See generally* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1473–75 (2000) (explaining the erosion of privacy laws in the healthcare sector and in general).

A. Openness and Transparency

Patients and consumers should know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them. Individuals must know how to exercise control. Laws, transparency, and openness do little to enhance patient control if they cannot find their PHI and control who has access to that information. Thus, under a NHIN, it will not be enough for individuals to have a PHR that they control; they will need to have greater access and control over their EHR.

B. Purpose Specification

The purposes for which PHI are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes, or others that are specified on each occasion of change of purpose. Such limitations would require the informed consent of individuals for a change of purpose. This, of course, is what HIPAA fails to do.

C. Collection Limitation

PHI should only be collected for specified purposes and should be obtained by lawful and fair means. The collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. Where possible, individuals should have knowledge of data collection or provide consent for collections.

D. Individual Participation and Control

Individuals should be able to control access to their personal information. They should know who is storing what information and how that information is used. They should also be able to review the way their information is being used or stored.

E. Data Quality and Security Safeguards

All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date. Reasonable safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure. As early as 2000, the National Research Council (NRC) recommended that the federal government take steps to include new *technical features* that will better protect the privacy and anonymity of Internet users.[91] Features identified by the NRC include the use of electronic

91. NAT'L RESEARCH COUNCIL, NETWORKING HEALTH: PRESCRIPTIONS FOR THE INTERNET 235–68 (2000).

passwords,[92] firewalls,[93] digital signatures,[94] time and date stamps,[95] and encryption software[96] that allows patient health information to be encoded and decoded for transmission and storage. According to the NRC, "the features include mechanisms to protect the anonymity of Internet users, to keep patient information secure, to validate the identity of users participating in confidential online transactions, and to track users of databases."[97]

F. Accountability and Oversight

Entities in control of PHI must be held accountable for implementing these principles. An oversight body should be created that is comprised of all stakeholders, including representatives of government, the health care industry, vendors and technologists, and consumer, privacy and patient advocates. The oversight body would monitor the effectiveness of the system in accomplishing its goal of benefiting health care. It would also review compliance issues and stay current with problems that arise.

G. Remedies and Sanctions

Under the NHIN, patients should have a right of action for any damages that result from mishandling of their PHI. Remedies and sanctions must exist to address security breaches or privacy violations. The problem is that it is often very difficult to determine who is responsible for a privacy violation. For example, almost 50 percent of individuals who are victims of identity theft are unable to determine who stole their personal information.[98] Although difficult to enforce, there still ought to be minimum punishments for those individuals who violate the PHI of others.

As mentioned above, these seven privacy principles are derived from existing laws, statutes, and fair information practices. There is, therefore, nothing really new about them. What is new and significant is that there is a reduction in the number of covered entities that have access to PHI, and more individual control over how, when, and what PHI will be disclosed and used. The success of these improvements, however, depends upon their effective application and enforcement.

---

92. *Id.* at 63–65.

93. *Id.* at 147–50.

94. *Id.* at 79–80.

95. *Id.* at 117.

96. *Id.* at 63–65.

97. Vincent Kiernan, *Medicine Could Benefit from Internet Improvement, Report Says*, CHRON. HIGHER EDUC., Feb. 24, 2000 (citing NAT'L RESEARCH COUNCIL, *supra* note 91, at 256).

98. Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection (Version 2.0)* 21 (Geo. Wash. Univ. Law Sch., Pub. Law Research Paper No. 59, 2005), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=699701 (follow "download" hyperlink).

CONCLUSION

E-medicine provides some very real benefits for our healthcare system, including reduced costs, increased access to services and providers,[99] and reductions in medical errors.[100] These benefits, however, should not blind us to the potential risks of e-medicine, in particular, privacy violations, unauthorized use and disclosure of PHI, and erosion in the public's trust of our health care system. Therefore, it is absolutely essential that future privacy regulations significantly reduce the number of entities that have legal and authorized access to PHI as well as provide individuals greater access and control over their PHI. It is also necessary that adequate security measures be implemented in order to minimize the risk of unauthorized access to the PHI.

Also, the creation of a NHIN will make it easier for authorized individuals to access patients' PHI data. The problem is that a network that can be utilized more easily by authorized individuals anytime and anywhere is a network that potentially makes it easier for unauthorized individuals to breach the privacy and confidentiality of PHI. Legislation and technology can do much to minimize privacy risks, but the human factor is also vitally important. Health care professionals need to be trained in the use of EHRs and related digital technologies and need to understand the ethical significance of and justifications for maintaining the privacy and confidential PHI, as well as the implications of its misuse. If not, then it is unlikely that PHI will remain private for very long.

99. Keith A. Bauer, *Distributive Justice and Rural Healthcare: A Case for E-Health*, 17 INT. J. APPLIED PHIL. 243–54 (2003).

100. *See* Keith A. Bauer, *Using the Internet to Empower Patients and to Develop Partnerships with Clinicians*, AM. J. BIOETHICS, Dec. 2001, at W2.