ENSURING THE PRIVACY AND CONFIDENTIALITY OF ELECTRONIC HEALTH RECORDS†

*Nicolas P. Terry**
*Leslie P. Francis***

In 2004, President Bush announced his plan to ensure that most Americans would have electronic health records within ten years. Although substantial progress has been made toward achieving that goal, this progress has primarily reflected institutional interests and priorities by focusing on system architecture and technical standards. This article argues that in order for a nationwide transition to electronic medical records to be successful, however, the system must receive acceptance from patients and physicians. Thus, it must address and protect issues at the forefront of their concerns: namely, privacy and confidentiality. Instead of merely adopting the minimal protections afforded by HIPAA, the electronic health records system must embrace an autonomy-based, default position of full patient control over personal information, with very limited exceptions. Consequently, hard choices must be made as to the architectural and patient consent models that may involve subjugating some interoperability and comprehensiveness ambitions to principled protections of patient autonomy.

I. INTRODUCTION

On April 26, 2004, President Bush announced his plan to ensure that most Americans would have electronic health records within ten years.[1] Although some technical and many financial issues remain, there

* Chester A. Myers Professor of Law, Co-Director, Center for Health Law Studies, Professor of Health Management & Policy, Saint Louis University, e-mail: terry@slu.edu. I thank Michael Henderson, SLU J.D. candidate 2007, for his most helpful editorial suggestions.

** Professor and Chair, Department of Philosophy, Alfred C. Emery Professor of Law, University of Utah, e-mail: francisl@law.utah.edu.

1. THE WHITE HOUSE, TRANSFORMING HEALTH CARE: THE PRESIDENT'S HEALTH INFORMATION TECHNOLOGY PLAN, http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html (last visited Oct. 3, 2006). A more generalized commitment was announced in the 2006 State of the Union Address: "We will make wider use of electronic records and other health in-

has been substantial progress towards this goal. The project has now reached the point where acceptance by patients and physicians is crucial. In the health information technology (HIT) domain, the interests of patients and physicians do not always coincide;[2] patients tend to want more connectivity and online service from their physicians, while physicians are still ambivalent about technologically mediated care.[3] However, physicians and patients share common ground over many of the confidentiality and privacy issues raised by electronic health records (EHRs).

To date, the Bush administration has framed the EHR privacy-confidentiality issue quite narrowly, identifying only divergent state laws as creating barriers to successful implementation of its grand scheme. In fact, the issue runs far deeper.[4] In our view, the proposed national EHR system creates some fundamental privacy-confidentiality issues that must be satisfactorily resolved prior to implementation. Patients who lack trust in the national EHR system will opt out or frustrate many of the system's goals by hiding information from their physicians. Equally, physicians who perceive the new system as inconsistent with their professional standards of confidentiality or as creating liability "traps" will avoid participation or, if given no choice, will reduce or distort their charting.

formation technology, to help control costs and reduce dangerous medical errors." President George W. Bush, State of the Union Address (Jan. 31, 2006) (transcript available at http://www.whitehouse.gov/news/releases/2006/01/20060131-10.html).

2. *See generally* Nicolas P. Terry, *Prescriptions sans Frontières (or How I Stopped Worrying about Viagra on the Web but Grew Concerned about the Future of Healthcare Delivery)*, 4 YALE J. HEALTH POL'Y L. & ETHICS 183, 226–32 (2004).

3. *See Health Information Technology Activities at the Agency for Healthcare Research and Quality: Hearing Before the S. Comm. on Commerce, Science, and Transportation Subcomm. on Technology, Innovation, and Competitiveness*, 109th Cong. 2, 6 (2005) (statement of Carolyn M. Clancy, M.D., Director, Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services) ("Unlike the baseball field in the movie Field of Dreams [sic], we have dramatic examples of the building of health IT systems, whose designers found physicians and other clinicians neither came nor played."); *see also* Robert G. Brooks & Nir Menachemi, *Physicians' Use of Email With Patients: Factors Influencing Electronic Communication and Adherence to Best Practices*, J. MED. INTERNET RES., Jan.–Mar. 2006, *available at* http://www.jmir.org/2006/1/e2/ (survey reporting only modest advances in the adoption of e-mail communication with patients by physicians); Wall Street Journal Online/Harris Interactive Health-Care Poll, Few Patients Use or Have Access to Online Services for Communicating with their Doctors, but Most Would Like To, Sept. 22, 2006, http://www.harrisinteractive.com/news/newsletters/wsjhealthnews/WSJOnline_HI_Health-CarePoll2006vol5_iss16.pdf (finding that large majority of adults would like e-mail reminders and online appointment scheduling and that a majority of patients consider the offer of such services as a discriminator in choosing a provider).

4. One issued Request for Proposal on "Privacy and Security Solutions for Health Information Exchange" focuses on the need "to assess and develop solutions to address state and business privacy and security practices that may pose challenges to interoperable health information exchange." U.S. Dep't of Health & Human Servs., Fact Sheet: Health Information Technology Requests for Proposals (June 6, 2005), http://www.os.dhhs.gov/healthit/documents/RFPfactsheet.pdf [hereinafter Fact Sheet]. This resulted in a $11.5 million contract awarded to Privacy and Security Solutions to study the issue. Press Release, U.S. Dep't of Health & Human Servs., HHS Awards Contracts to Advance Nationwide Interoperable Health Information Technology (Oct. 6, 2005), *available at* http://www.hhs.gov/news/press/2005press/20051006a.html.

There are great advantages to using electronic records more extensively, both within the offices of individual providers, where they are known as electronic medical records (EMRs), and also when such records are linked across multiple providers, in which case they are known as electronic health records (EHRs). One obvious advantage is clarity. Electronic records are far more readable than handwritten documents stored in fading folders, allowing providers to avoid the low-hanging fruit of medical and medication errors. Another advantage is searchability: electronic records can be scanned for drug interactions or for consistent patterns of symptoms. They can also be matched with evidence-based protocols to discern treatment strategies that do not meet the standard of care or to recommend improved methods of patient management.

Moreover, in an EHR, records cease to exist in information silos, thus creating additional advantages over paper records. First, they are combined or interlinked to maximize coordination of care. Second, they offer enhanced accessibility: electronic records can be available to providers all over the country and the world, as mobile as the patients they describe. Finally, on a social level, EHRs are searchable for patterns of disease, prescription use (or abuse), treatment outcomes, or even the costs of therapy. These great benefits cannot be gainsaid.

At the same time, these advantages are threats. When inappropriate or false material is included in records, it will be persistent and reverberate in subsequent patient management decisions. Linkages may be drawn that violate patient requests for, or expectations of, confidentiality. EHRs may be searched in problematic ways. Records might be accessible to those who many believe should not have access to them (secondary users). Commercial entities may seek to add medical data to their other data holdings and sell the aggregated data for marketing or surveillance purposes. Groups might be targeted in epidemiological searches.

As a regional or national EHR becomes a technologically achievable goal with broad congressional support, we must distinguish the genuine advantages of EHRs from the deep problems they present and engineer the technical and legal models to minimize the problems. Yet, these are difficult tasks. Several possible EHR architectures and a myriad of patient choice models can be engineered. Worse, where the architectures and models fail to deal with the problems we identify, the legal and regulatory systems that should operate as surrogates themselves prove to be awkward or obstructive. In the United States, records law and privacy-confidentiality systems encompass both state and federal components. The United States does not have a robust track record in either conceptualizing or regulating health privacy.[5] Apparent federal solutions, such as the confidentiality regulations under the Health Insur-

5. James G. Hodge et al., *Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability*, 282 JAMA 1466, 1467–68 (1999).

ance Portability and Accountability Act of 1996 (HIPAA), are as sieve-like as they are incomprehensible.

Medical literature, opinion polls, United Kingdom and other foreign EHR implementations, and our own interactions suggest that patients and physicians are skeptical about the privacy, security, and safety of HIT systems. Consumers are told on a daily basis that their computers, when attached to networks, are pathologically insecure. Physicians continue to push back on safety technologies and remain deeply suspicious (even resentful) of the HIPAA transactional and patient privacy constructs.[6] Meanwhile, the media tirelessly report medical privacy horror stories of lost, stolen, or hacked records.[7]

A rational policymaker may view these stories as merely transitional or statistically insignificant aberrations. Yet public and professional perceptions of an EHR system are far different and potentially corrosive. The nature of such a system is difficult to convey to the public. A public perception of an EHR as a governmental "big brother" is increasingly likely. Take, for example, the views of the Association of American Physicians and Surgeons in a recent letter to Congress:

> Patients will definitely not benefit from this type of program because they do not control who has access to their sensitive identifiable medical records in any meaningful way. . . . [A] national health information system would effectively eliminate any and all patient consent to the release of their records by placing the records online. Patients would have virtually no control over who can sneak-a-peak at their very private and sensitive medical records.[8]

6. *Electronic Health Records and Privacy: Hearing Before the U.S. Dep't of Health and Human Servs. Nat'l Comm. on Vital and Health Statistics Subcomm. on Privacy*, 109th Cong. (2005) [hereinafter *Health Records Hearing*] (statement of Nicolas P. Terry).

7. *See, e.g.*, Nicolas P. Terry, *To HIPAA, a Son: Assessing the Technical, Conceptual, and Legal Frameworks for Patient Safety Information*, 12 WIDENER L. REV. 137 (2006); *Joplin Hospital Records Stolen from Company*, COLUM. DAILY TRIB. (Columbia, Mo.), July 25, 2005 (computers containing personal information of 27,000 patients stolen from microfilming company); *Hawaii Warns 43,000 Residents of Health Data Theft*, MOD. HEALTHCARE ONLINE, Apr. 14, 2006, http://www.modernhealthcare.com/news.cms?newsId=5039; Gary T. Kubota, *Hospital Loses Patient Data*, HONOLULU STAR BULL., Oct. 21, 2005, at A3 (hospital lost computer drive of personal information implicating 130,000 patients); Todd Milbourn, *Stolen Laptop Contains Files on HIV Patients*, SACRAMENTO BEE, Feb. 23, 2006, at B3 ("A laptop computer containing health information for 1,764 clients of CARES, a Sacramento HIV/AIDS clinic, was stolen during a home burglary."); Sean Webby, *Medical Records Theft Alarms Parents*, MERCURY NEWS (San Jose, Cal.), Sept. 20, 2005, at 1B (theft of records from Palo Alto nonprofit that works with emotionally troubled and developmentally challenged children); *Update: Thief Nabs Backup Data on 365,000 Patients*, COMPUTERWORLD, Jan. 26, 2006, http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,108101,00.html (theft of generally unencrypted computer backup data on 365,000 hospice and home healthcare patients in Oregon and Washington from employee's care); Press Release, Providence Health Sys. in Or., State Finds Providence Acted Appropriately Following Theft of Computer Disks, Tapes, *available at* http://www.providence.org/oregon/hcs/newsrelease.htm.

8. Letter from Jane M. Orient, M.D., Executive Director, Ass'n of Am. Physicians & Surgeons, to Congress (Feb. 2, 2006), *available at* http://www.aapsonline.org/confiden/hr4157-letter.php; *see also* Press Release, Institute for Health Freedom, Congress Could Vote Soon on a Bill that Abolishes State Health-Privacy Rights (Feb. 8, 2006), *available at* http://www.forhealthfreedom.org/Publications/Privacy/ActNowHR4157.html.

This article is premised on the end of one important phase in the development of a national electronic interoperable health records (EIHR) system: the satisfactory near completion of the technical specifications for infrastructure and data exchange.[9] As this "insider baseball" phase concludes, the "outside" stakeholders must be identified and satisfied. For a national EIHR system, cost[10] and lack of confidentiality are the two potential deal-breakers. This article addresses the second of these: the question of whether such an ambitious EIHR system can operate within a framework of ethically and practically satisfactory confidentiality, privacy, and security protections. Here, we analyze the possible EHR architectures and compare their implications for confidentiality, privacy, and security. Similarly, we examine the possible models of patient choice that can be integrated into such systems. Finally, we discuss what legal and regulatory steps will be required to provide privacy and confidentiality protections.

II. THE ROAD TO INTEROPERABLE HEALTH RECORDS

A. Technologies and Terminology

The HIT movement assaults us with a bewildering array of terminology expressed in "insider" acronyms.[11] Records technologies have their own confusing labels. In this article, we discuss several electronic records technologies. The most generalized label is EMR, which describes any form of computerized record-keeping, from a modest software package used in a single doctor's office to an enterprisewide, database-driven application. Primarily, however, this article concerns the EHR, a type of EMR architecture that permits the sharing of patient data among healthcare providers.

Some EHRs are conceptually and technically quite simple. For example, the personal EHR (PHR) is a database of medical information that is collected and maintained by the individual patient.[12] However, the EHR label is most often applied to far more complex systems that

9. *See, e.g.*, Consolidated Health Informatics (CHI) Initiative; Health Care and Vocabulary Standards for Use in Federal Health Information Technology Systems, 70 Fed. Reg. 76,287 (Dec. 23, 2005); *FDA Selects SNOMED for Drug Labels*, GOV'T HEALTH IT, Apr. 21, 2006, *available at* http://govhealthit.com/article94147-04-21-06-Web. *See generally* ELEC. HEALTH RECORD VENDORS ASS'N (EHRVA), EHRVA INTEROPERABILITY ROADMAP VERSION 2.0 (2006), http://www.himssehrva.org/docs/roadmap_v2.pdf.

10. For a summary of some of the financial issues, see *infra* text accompanying note 20.

11. Examples include Radio Frequency Identification (RFID), Computerized Order Entry appliances (CPOEs), and Clinical Decision-Support Systems (CDSS). *See generally* Terry, *supra* note 7.

12. *E.g.*, CapMed's Personal Health Record, http://www.capmed.com/products.html; iHealthRecord, http://www.ihealthrecord.org/; MyMedicalRecords.com, http://www.MyMedicalRecords.com. *See generally* Julie Appleby, *Don't Let Hurricanes Blow Your Medical Records Away*, USA TODAY, Oct. 27, 2005, at B1 ("Backers of direct-to-consumer online medical records say their services will gain ground, spurred by concern about record losses in disasters, the desire by consumers for more ease in moving medical records from one doctor to another and by the growing push to create a more digitized medical system.").

rely on technical interoperability between diverse electronic records systems. The federal government is primarily interested in a fully interoperable, longitudinal records system that will initially operate on regional networks (Regional Health Information Organizations, or RHIOs) before transitioning to a National Health Information Network (NHIN).[13] Due to scale and architecture, these models reduce or eliminate patient involvement in the sharing process.

B. The Bush Administration's EIHR Plan

Concomitant with his 2004 announcement that most Americans should have electronic health records within the next ten years, President Bush appointed Dr. David Brailer to a new post of National Health Information Technology Coordinator (ONCHIT) to guide the "nationwide implementation of interoperable health information technology."[14] ONCHIT has built on the previous work of NCVHS[15] and the Consolidated Health Informatics (CHI) Initiative[16] and oversees the Federal Health Architecture.[17]

The Bush administration publicly eschews any regulatory mandate directing healthcare providers to adopt EHRs.[18] Rather, it espouses EHR adoption via "a smooth market-led way."[19] Of course, with no government-funded mandate, there remain significant technical, cultural, and, particularly, financial[20] barriers to EHR adoption in addition to the

13. *See generally* H.R. 4859, 109th Cong. (2004); H.R. 4157, 109th Cong. (2004).

14. Exec. Order No. 13,335, 69 Fed. Reg. 24,059, § 3 (Apr. 30, 2004).

15. U.S. Dep't of Health & Human Servs., National Committee on Vital Health Statistics, http://www.ncvhs.hhs.gov (last visited Oct. 15, 2006).

16. U.S. Dep't of Health & Human Servs., Office of the National Coordinator for Health Information Technology, http://www.hhs.gov/healthit/chiinitiative.html (last visited Jan. 3, 2007).

17. U.S. Dep't of Health & Human Servs., Federal Health Architecture (FHA), http://www.hhs.gov/fedhealtharch (last visited Jan. 3, 2007) ("The FHA is managed within the Office of the National Coordination for Health IT . . . .").

18. Chris Murphy & Marianne Kolbasuk McGee, *Industry Must Improve Its Technology*, INFORMATIONWEEK, June 21, 2004, at 30 ("I don't want to see a Son of HIPAA put into law." (quoting David Brailer, Coordinator, Nat'l Healthcare Info. Tech., Speech to the National Alliance for Health Information Technology)).

19. Press Release, U.S. Dep't of Health & Human Servs., *Secretary Leavitt Takes New Steps to Advance Health IT* (June 6, 2005), *available at* http://www.os.dhhs.gov/news/press/2005pres/20050606.html.

20. The core issue is the misalignment of incentives such that, basically, there is an inverse relationship between those required to invest in EMR/EHR and those who would benefit. *See* Joan S. Ash & David W. Bates, Position Paper, *Factors and Forces Affecting EHR System Adoption: Report of a 2004 ACMI Discussion*, 12 J. AM. MED. INFORM. ASS'N 8, 10 (2005), *available at* http://www.jamia.org/cgi/reprint/12/1/8; Michael W. Bender, Ahmed H. Mitwalli, & Steven J. Van Kuiken, *What's Holding Back Online Medical Data*, MCKINSEY Q., Dec. 2005, http://mckinseyquarterly.com/article_print.aspx?L2=12&L3=63&ar=1699; Terry, *supra* note 7, at 173–84; *see also* Nancy Ferris, *Doctors Want Payment Boost for Using e-Health Records*, Gov't Health IT, Jan. 31, 2006, *available at* http://govhealthit.com/article92155-01-31-06-Web (detailing American College of Physicians' call for Medicare to reimburse primary care physicians for using EHRs); Christopher Rowland, *Digital Divide Widens in Medicine: Computerized Records Improve Care but Some Doctors Can't Afford It*, BOSTON GLOBE, Feb. 10, 2006, at C1, *available at* http://www.boston.com/business/technology/articles/2006/02/10/digital_divide_widens_in_medicine/?page=full.

confidentiality-privacy issues raised in this article.[21] Notwithstanding, ONCHIT and its supporters have moved inextricably towards the most complex, professionally disruptive, and, at $400 billion,[22] the most expensive EHR architecture.[23] Current ONCHIT request for proposals (RFPs) address technical standards, the certification of EMR systems (to guarantee interoperability), and most crucially, prototyping an internet-based NHIN architecture.[24] Not surprisingly, a NHIN (or multiple RHIO) architecture also provides the greatest challenge to protecting patient confidentiality, privacy, and security.

C. Alternative Models

Although the administration has not entered into a public debate over its preferred EHR architecture, there are several alternatives to a fully interoperable electronic record either in use or under development in the United States and further afield. Some of these architectures have different confidentiality and privacy implications, though they may also lack some of the error-reduction and outcomes research benefits of a national EIHR.

1. United States

Within the United States, two major alternatives to a fully interoperable EHR architecture have emerged: Continuity of Care Records and Personal EHRs. The Continuity of Care Record (CCR) is an effort to standardize electronic records to ease portability.[25] A specification developed by the Health Information Management and Systems Society (HIMSS) and various professional bodies,[26] CCR aims to extract data from existing proprietary EMR systems and export it to a common text

21. *See* discussion *infra* Part III.B.

22. Rainu Kaushal et al., *The Costs of a National Health Information Network*, 143 ANNALS OF INTERNAL MEDICINE 165, 165 (2005). In contrast to the expected costs, the 2007 proposed federal budget contains $116 million for the Office of the National Coordinator, $50 million for the Agency for Healthcare Research and Quality, and $3 million for the Office of the Assistant Secretary for Planning and Evaluation. *See* OFFICE OF MGMT. AND BUDGET, BUDGET OF THE UNITED STATES GOVERNMENT: FISCAL YEAR 2007, at 109 (2006), *available at* http://www.whitehouse.gov/omb/budget/fy2007/pdf/budget/hhs.pdf.

23. *See generally* Press Release, U.S. Dep't of Health & Human Servs., Thompson Launches "Decade of Health Information Technology" (July 21, 2004), http://www.hhs.gov/news/press/2004pres/20040721a.html (explaining the general parameters of the federal HER plan).

24. Fact Sheet, *supra* note 4.

25. The current specification is E2369-05, Standard Specification for Continuity of Care Record (CCR). *See* ASTM International, http://www.astm.org/cgi-bin/SoftCart.exe/DATEBASE.CART.REDLINE_PAGES/E2369.htm?L+mystore+jjfs9503 (last visited Oct. 10, 2006); *see also* AAFP's Center for Health Information Technology, Essential Similarities and Differences Between the HL7 CDA/CRS and ASTM CCR, http://www.centerforhit.org/PreBuilt/chit_ccrhl7.pdf (last visited Jan. 3, 2007).

26. *See* Medical Records Institute, Continuity of Care Record (CCR), http://www.medrecinst.com/pages/about.asp?id=54 (last visited Jan. 3, 2007).

export format (XML[27]), which would allow portability of summary data[28] and enable it to be given to a patient or transferred directly to the patient's next provider.[29]

A PHR is a personal database of medical information that is collected and maintained by the patient, who controls whether and to what extent it is shared with providers.[30] PHRs are supplied free by, for example, employers or healthcare providers on a subscription basis. They may be web-based or databases created on the patient's own computer. Recently, the Center for Medicare and Medicaid Services (CMS) issued a request for information (RFI) seeking input on how best it should make data about Medicare beneficiaries available for incorporation into such personal EHRs.[31]

2. Outside the United States

National or regional EIHRs are also gaining attention in the healthcare systems of other developed countries. For example, in Canada, *Infoway*, a nonprofit partnership of federal, provincial, and territorial governments, is coordinating the deployment of a pan-Canadian EHR.[32] Currently, *Infoway* is emphasizing the development of technical interoperability standards.[33] New Zealand has announced a wide-ranging Health Information Strategy that includes interoperable EHR event summaries that can be distributed at local, regional, and national levels.[34] New Zealand has decided not to create a national EHR database.[35] The most advanced EIHR projects, however, are in the United Kingdom and Australia.

In 1998, the United Kingdom commenced an ambitious and costly information technology-based makeover of its entire healthcare system. This *National Programme for IT in the NHS* (NPfIT) involved the in-

27. *See generally* World Wide Web Consortium, Extensible Markup Language (XML), http://www.w3.org/XML/ (last visited Oct. 3, 2006).

28. Medical Records Institute, s*upra* note 26.

29. *See* David C. Kibbe et al., *The Continuity of Care Record*, 70 AM. FAM. PHYSICIAN 1220, 1222 (2004).

30. Tracy D. Gunter & Nicolas P. Terry, *The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions*, J. MED. INTERNET RES., Jan.–Mar. 2005, *available at* http://www.jmir.org/2005/1/e3; *see e.g.*, CapMed's Personal Health Record, *supra* note 12; iHealthRecord, *supra* note 12. *See generally* Laura Landro, *High-Tech Tools Help Patients Manage Own Medical Records*, DESERET NEWS (Salt Lake City, Utah), Feb. 28, 2005, at C1.

31. Federal Business Opportunities, Synopsis of Request for Information-Centers for Medicare & Medicaid Services' Role in Personal Health Records (July 18, 2005), http://www.fbo.gov/servlet/Documents/R/1233397.

32. Canada Health Infoway, Overview, http://www.infoway-inforoute.ca/en/WhatWeDo/Overview.aspx (last visited Jan. 3, 2007).

33. Canada Health Infoway, Infoway Standards Collaboration Process, http://www.infoway-inforoute.ca/en/WhatWeDo/StandardsCollaboration.aspx (last visited Oct. 3, 2006).

34. NEW ZEALAND MINISTRY OF HEALTH, HEALTH INFORMATION STRATEGY FOR NEW ZEALAND 2005 (2005), *available at* http://www.moh.govt.nz/moh.nsf/0/1912064EEFEC8EBCCC2570430003DAD1/$File/health-information-strategy.pdf.

35. *See id.*

vestment of some $11.1 billion over a ten-year program.[36] The *NHS Information Authority* originally led the United Kingdom program, but after critical reviews, it was renamed *NHS Connecting for Health*[37] and is now directly overseen by the Department of Health.[38] A key component of the U.K. program is the NHS Care Records Service (NHS CRS), which aims to provide an electronic NHS Care Record for all U.K. patients. Although the first fully electronic transfer of a patient record between doctors' offices occurred in November 2005,[39] organizational, cultural, and financial woes have slowed considerably the EHR program in the United Kingdom.[40] Both providers and patients have seriously criticized the EHR program because of privacy and security concerns.[41]

The Australian *HealthConnect* system has completed its initial trials, but recent funding problems and questions about privacy and consent issues have slowed progress.[42] These delays have occurred despite the fact that the *HealthConnect* model supports a robust health confidentiality-privacy system[43] by both pushing only "event summaries" to the centralized EIHR and providing for considerable patient data carveouts designed to keep certain data within patient control.[44]

First, *HealthConnect* does not create a true longitudinal record, but aggregates elements extracted from a patient's existing EMR(s).[45] These event summaries are defined as "an electronic overview of a visit to a doctor or hospital, or some other health care event . . . contain[ing] only

36. *See* Editorial, *National Programme for Information Technology Is Sorely Needed and Must Succeed—but Is off to a Shaky Start*, 328 BMJ 1145, 1145 (2004).

37. History of Our Organisation—NHS Connecting for Health, http://www.connectingforhealth.nhs.uk/about/history (last visited Nov. 10, 2006).

38. *Id.*

39. NHS Connecting for Health Completes Transfer of a Patient's Medical Record, EGOV MONITOR, Nov. 8, 2005, http://www.egovmonitor.com/node/3454 (last visited Oct. 12, 2006).

40. *See* Jane Hendy et al, *Challenges to Implementing the National Programme for Information Technology (NPfIT): A Qualitative Study*, 331 BMJ 331, 332–34 (2005); *see also* Brian Robinson, *U.K. Lacks Support for Health IT Modernization*, GOV'T HEALTH IT, Jan. 12, 2006, *available at* http://www.govhealthit.com/article91953-01-12-06-Web (reporting that nearly 70% of the doctors surveyed said they would have insufficient funds to properly implement NPfIT, while only 30% of doctors view the program an important priority for the NHS); Nicholas Timmins, *NHS and Suppliers Struggle With Basics on Patient Record System*, FIN. TIMES UK, Nov. 1, 2006, *available at* 2006 WLNR 18981715.

41. *See Call for Review of NHS IT Upgrade*, BBC NEWS, Apr. 10, 2006, http://news.bbc.co.uk/1/hi/health/4896198.stm; *GPs Fret over Online Records*, TIMES (London), June 7, 2005, Public Agenda, at 6; Alice Miles, *The Spy in the GP's Surgery*, TIMES (London), Jan. 12, 2005, at 18; Helene Mulholdland, *NHS Set to Miss e-Booking Target*, GUARDIAN UNLIMITED, Sept. 30, 2005, http://www.guardian.co.uk/uknews/story/0,16559,1582117,00.html; Nicholas Timmins, *Doctors' Debate Delays Patient Record*, FIN. TIMES UK, Apr. 27, 2006, *available at* 2006 WLNR 7068306 (describing additional delays as doctors favor opt-in model); Nick Triggle, *Confidentiality Fear over Records*, BBC NEWS, June 29, 2005, http://news.bbc.co.uk/2/hi/health/4633213.stm; *see also infra* text accompanying note 272.

42. Karen Dearne, *Feds' Health Data Project Stalls*, AUSTRALIAN, June 7, 2005, at 29.

43. *See* Australian Government, Office of the Privacy Commissioner, Health, http://www.privacy.gov.au/health/index.html (last visited Jan. 3, 2007).

44. Nicolas P. Terry, *Electronic Health Records: International, Structural and Legal Perspectives*, 12 J.L. & MED. 26, 33 (2004).

45. *Id.* at 32–33.

the information that is relevant to the future health and care of the consumer, rather than the comprehensive notes that a doctor may keep . . . ."[46] Additionally, *HealthConnect* utilizes a "push" model, whereby data is sent from the local EMR to a centralized *HealthConnect* record, in contrast to the proposed U.S. EIHR model that seems likely to adopt a "pull" model, whereby the centralized system initiates a data request from a provider's record using a data pointer.[47] Finally, *HealthConnect* not only creates an event summary that is less than a complete record, but it also allows the patient (in consultation with the physician) to control what data are included and who may view it.[48]

Because of an apparent reduction in Commonwealth (federal) funding, *HealthConnect* may evolve into a decentralized[49] and less EHR-centric project.[50] While many Australian patients and physicians have articulated a preference for simple consent models such as a generalized "opt-in" and prospective consent for the pushing of their data to the centralized *HealthConnect* summary record, many remain uncomfortable with any participation in the system.[51]

3. RHIOs and the NHIN

ONCHIT is publicly encouraging and, to an extent, incentivizing RHIOs while at the same time designing a NHIN.[52] The fundamental feature of both RHIOs and a NHIN is that they are not intrinsically electronic records, but networking infrastructures that facilitate interconnectivity between existing systems.[53] As such, these systems are premised not only on the widespread deployment of EMR and EHR systems in medical offices, hospitals, and hospital systems, but also on the ability of

46. HealthConnect, Event Summaries, http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/event-summaries (last visited Oct. 12, 2006).

47. HealthConnect, Privacy, http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/privacy (last visited Oct. 3, 2006).

48. *Id.*

49. *See, e.g.*, Karen Dearne, *Seniors Corralled for Pilot*, AUSTRALIAN IT, Mar. 23, 2006 (on file with author) (detailing New South Wales' Health's "shaky start" to trial of a HealthConnect-style electronic record pilot, Healthelink, using an automatic enrollment, opt-out model).

50. *See generally* HealthConnect Implementation Strategy, Version 2.0 (rev.), June 2005, http://www.healthconnect.gov.au/pdf/implementation.pdf.

51. COMMONWEALTH OF AUSTL., LESSONS LEARNED FROM THE MEDI*CONNECT* FIELD TEST AND HEALTH*CONNECT* TRIALS 8 (2005), *available at* http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/key-reports (follow "Lessons Learned form the Medi*Connect* Field Test and Health*Connect* Trials 1–10" hyperlink).

52. *See, e.g.*, Press Release, U.S. Dep't of Health & Human Servs., HHS Awards Contracts to Develop Nationwide Health Information Network (Nov. 10, 2005), *available at* http://www.hhs.gov/news/press/2005pres/20051110.html.

53. The NHIN concept may grow closer to a national EHR if it utilizes a centralized data warehouse rather than a pointer system. It is, however, unlikely that the federal government would be prepared to finance such a centralized model.

those deployed local systems to interconnect with the network. Neither of those predicates is true.[54]

Even leaving aside the cultural, professional, legal,[55] and financial disincentives to electronic records, interoperable systems face something of a catch-22: RHIOs and the NHIN cannot be built without local EMR or EHR systems, but providers are hesitant to commit to local systems without knowing the RHIO or NHIN to which they may connect. Providers considering involvement in a RHIO additionally face the question of what will happen to their RHIO if, subsequently, a NHIN is constructed.[56]

III. WEIGHING THE COSTS AND BENEFITS

Many potential benefits of interconnected EHRs seem easily measurable: improved continuity of care, reduced frequency of errors in medication and treatment, and increased potential for outcomes research and public health surveillance.[57] Beyond implementation costs, other costs are more intangible: privacy, confidentiality, and security risks; and concerns about the behavior of patients who, wary of the implications of electronic records, attempt to keep their records, or even themselves, out of the healthcare system altogether. These costs are significant, and addressing them by system design at the outset may be necessary to generate the trust in networked EHRs that will enable achievement of their very substantial benefits. If, for example, concerns about security risks result in an architecture that does not permit records to be searchable as part of a common database, opportunities for performance evaluation, outcomes research, and public health surveillance will be lost.[58]

A. Benefits and Drivers

"At its most sophisticated or most infused level, the EHR becomes a hub of all activity, something that permeates every element of the

54. *See, e.g.*, Ford et al., *Predicting the Adoption of Electronic Health Records by Physicians: When Will Health Care be Paperless?*, 13 J. AM. MED. INFORMATICS ASS'N 106, 108–10 (2006) (concluding that universal EMR/EHR adoption will not be met by 2014 and suggesting a conservative estimate that 86.6% of physicians in small practices will be using EHRs in 2024).

55. *See generally* Terry, *supra* note 7, at 160.

56. *See* Joseph Goedert, *Are RHIOs for Real?*, HEALTH DATA MGMT., Feb. 6, 2006, at 44, 45.

57. *See, e.g.*, RAND CORP., HEALTH INFORMATION TECHNOLOGY: CAN HIT LOWER COSTS AND IMPROVE QUALITY? (2005), http://www.rand.org/pubs/research_briefs/RB9136/RAND_RB9136.pdf.

58. For a summary of these benefits, costs, and strategies, see Letter Report from Simon P. Cohn, Chairman, Nat'l Comm. on Vital and Health Statistics, to Michael O. Leavitt, Secretary, U.S. Dep't of Health & Human Servs. (Sept. 9, 2005), *available at* http://www.ncvhs.hhs.gov/50909lt.htm. For a discussion of the tensions concerning privacy, security, and proprietary information in system design, see Kenneth D. Mandl, Peter Szolovits & Isaac S. Kohane, *Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private*, 322 BMJ 283 (2001).

workflow and of work life."[59] Although this characterization is somewhat hyperbolic, a comprehensive, longitudinal EHR ideally will: (1) interconnect with and enhance other error-reducing and cost-saving technologies such as decision support systems; (2) streamline healthcare dataflow using an interoperable and standardized nomenclature; (3) improve quality of care by encouraging accurate, timely, and legible communication among providers; (4) automate adverse event and medical error disclosure; and (5) facilitate reliable and reproducible outcomes research and reporting, as well as other public health initiatives.[60]

One of the most discussed benefits of EHRs is the potential for error reduction. In an electronic format, data are legible, thus minimizing the risks of pharmacists misreading handwriting on prescriptions or subsequent providers struggling to decipher records of earlier treatment. Data are also directly transferable, thus avoiding transcription errors and delays in recording prescriptions or test results communicated by telephone.[61] Functions can be written to flag prior allergic reactions, drug interactions, or other contraindications for contemplated therapy, thus additionally reducing the potential for error.[62] Computerized provider order entry systems (CPOEs) linked to EHRs may reduce the incidence of medication errors.[63] These apparent advantages, however, are not uncontroversial; there may be risks of additional adverse events, particularly as electronic systems are introduced, and there is much discussion in the literature about how to reduce unanticipated errors due to human/technology interfaces.[64]

59. *See* Ash & Bates, *supra* note 20.

60. Gunter & Terry, *supra* note 30.

61. Jan Walker et al., *The Value of Health Care Information Exchange and Interoperability*, HEALTH AFF. (Jan. 19, 2005), http://content.healthaffairs.org/cgi/reprint/hlthaff.w5.10v1.pdf.

62. *E.g.* Nadir R. Shah et al., *Improving Acceptance of Computerized Prescribing Alerts in Ambulatory Care*, 13 J. AM. MED. INFO. ASS'N 5, 5 (2006); Robyn Tamblyn, *Improving Patient Safety Through Computerized Drug Management: The Devil Is in the Details*, 5 HEALTHCARE PAPERS 52, 54–56 (2004). For a discussion of the error-reduction potential of EHRs, see David A. Hyman & Charles Silver, *The Poor State of Health Care Quality in the U.S.: Is Malpractice Liability Part of the Problem or Part of the Solution?*, 90 CORNELL L. REV. 893 (2005). For an overview of the potential cost effectiveness of electronic records systems, see Sarah Klein, *Issue of the Month: Who Has $400 Billion to Build a National Health Information Network?*, QUALITY MATTERS: SEPTEMBER UPDATE FROM THE COMMONWEALTH FUND, Sept. 2005, *available at* http://www.cmwf.org/publications/publications_show.htm?doc_id=294918. The Massachusetts eHealth Collaborative and the Massachusetts Medical Society have just begun a demonstration of the use of EHRs in the offices of physicians. Press Release, Mass. e-Health Collaborative, Massachusetts Takes a Giant Step Towards Electronic Health Records (Oct. 5, 2005), *available at* http://www.maehc.org/documents/HIMMSE-HEALTHfinal_000.pdf. Many healthcare systems have significant experience with electronic records, including the Veterans Health Administration, the New England Healthcare Electronic Data Interchange Network, the Indiana Network for Patient Care, the Santa Barbara County Care Data Exchange, the Patient Safety Institute's National Benefit Trust Network, and the Markle Foundation's Healthcare Collaborative Network, Kelsey D. Patterson, *Healing Health Care: Fixing a Broken System with Information Technology*, 14 KAN. J.L. & PUB. POL'Y 193, 200 (2004).

63. Anne Bobb et al., *The Epidemiology of Prescribing Errors: The Potential Impact of Computerized Prescriber Order Entry*, 164 ARCHIVES INTERNAL MED. 785, 789–90 (2004).

64. *E.g.*, Margaret Caudill-Slosberg & William B. Weeks, *Case Study: Identifying Potential Problems at the Human/Technical Interface in Complex Clinical Systems*, 20 AM. J. MED. QUALITY 353

An electronic format also permits entries in patients' records to be checked against programmed guidelines and clinical decision support systems, prompting providers if prescription amounts are out of range, if necessary data have been omitted in the record, or if recommended procedures have not been performed.[65] Here, too, there is some dispute about whether use of these support systems will improve outcomes for patients.[66]

To be sure, these benefits depend on accurate data entry into the electronic record, but even here, electronic records may have advantages over paper records. Some data, such as laboratory test results or digitized scans, can be entered into a record automatically. Software monitoring electronic records can be programmed to flag unusual or inconsistent entries, from a blood pressure or prostrate-specific antigen (PSA) reading much higher or lower than before, to a shift in noted patterns of calcification in a mammography reading.[67] Patients who have access to their EHRs, which are more easily transmitted and more portable than paper copies, can also check them for accuracy, just as they can perform online reviews of credit card or banking statements.

Other potential advantages of electronic records in patient care are patient education and communication. Physicians or patients can use electronic records to graph progress in easily visualized ways.[68] Electronic record systems can be programmed to send patients e-mail reminders for follow-up care. Electronically generated letters or e-mails can be used to contact patients if new and relevant information becomes

(2005); Yong Y. Han et al., *Unexpected Increased Mortality After Implementation of a Commercially Sold Computerized Physician Order Entry System*, 116 PEDIATRICS 1506 (2005); Ross Koppel et al., *Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors*, 293 JAMA 1197 (2005); Jonathon R. Nebeker et al., *High Rates of Adverse Drug Events in a Highly Computerized Hospital*, 165 ARCHIVES INTERNAL MED. 1111 (2005). For a response, see Press Release, The Leapfrog Group, Leapfrog Responds to University of Pennsylvania Study on CPOE Errors (Mar. 10, 2005), *available at* http://www.leapfroggroup.org/media/file/Leapfrog_on_UPenn.CPOE_study.pdf.

65. *E.g.*, Vahid Ebrahiminia et al., *Representing the Patient's Therapeutic History in Medical Records and in Guideline Recommendations for Chronic Diseases Using a Unique Model*, 116 STUD. HEALTH TECH. INFORMATICS 101 (2005) (diabetes management); Steven Ornstein et al., *A Multimethod Quality Improvement Intervention to Improve Preventive Cardiovascular Care: A Cluster Randomized Trial*, 141 MED. 523 (2005) (quality indicators for cardiac disease prevention); Matthew H. Samore et al., *Clinical Decision Support and Appropriateness of Antimicrobial Prescribing: A Randomized Trial*, 294 JAMA 2305 (2005) (finding significant decline in antibiotic prescriptions for upper respiratory infections in communities using CDSS system).

66. William M. Tierney et al., *Can Computer-Generated Evidence-Based Care Suggestions Enhance Evidence-Based Management of Asthma and Chronic Obstructive Pulmonary Disease? A Randomized, Controlled Trial*, 40 HEALTH SERVICES RES. 477, 477 (2005) (finding no relation between care prompts and patient management in a randomized trial of electronic care prompts in asthma patients).

67. For a discussion of these benefits in the VistA system developed by the Veteran Health Administration, see Jonathan B. Perlin et al., *The Veterans Health Administration: Quality, Value, Accountability, and Information as Transforming Strategies for Patient-Centered Care*, AM. J. MANAGED CARE, Nov. 2004, at 828, 832–36.

68. *See* Douglas McCarthy, *Case Study: Frontline Physicians and Their Patients Reap Benefits from EHRs*, QUALITY MATTERS: SEPTEMBER UPDATE FROM THE COMMONWEALTH FUND, Sept. 2005, http://www.cmwf.org/publications/publications_show.htm?doc_id=294918#casestudy.

available, if they are overdue for an appointment, or if medications are withdrawn from the market.[69] The advantages and disadvantages of provider-patient e-mail contact and web-based communication are increasingly discussed in the medical practice literature.[70] Perhaps more controversially, patients themselves use the web with increasing frequency to learn about health conditions, therapeutic alternatives, and care providers specializing in their conditions. Armed with their own EHRs, and guided by their physicians, patients may be able to make more informed use of this resource.[71]

Leaving aside the potential for the improvement of care at the level of the individual patient, several forces relating to healthcare delivery currently drive the U.S. interest in a national system of interoperable electronic records.[72] First, major shifts in care venues have accelerated the need for efficient flow of patient medical and billing information between organizationally and geographically distinct providers. Patients now are more likely to receive care in ambulatory care rather than inpatient settings. They are geographically mobile and also tend to change providers as their insurance or preferences change. If test results from prior treatment are readily available in an accurate and secure format, patients may avoid the inconvenience, risk, and expense of reduplicative testing that occurs when they see new providers who are unsure about reports of prior medical evaluations.[73]

Second, the operational aspects of managed care have increased the need for data transparency.[74] "Gate keeping" physicians who authorize referrals, third party payers who want pay-for-performance "report cards," and system administrators who need sophisticated utilization review and risk management tools all are served by electronic record sets.

69. For a description of some of these uses of EHRs in a primary care practice, see Richard J. Baron et al., *Electronic Health Records: Just Around the Corner? Or Just over the Cliff?*, 143 ANNALS INTERNAL MED. 222 (2005).

70. *E.g.*, Felicity Goodyear-Smith et al., *Pandora's Electronic Box: GPs Reflect upon Email Communication with Their Patients*, 13 INFORMATICS PRIMARY CARE 195 (2005); Steven J. Katz & Cheryl A. Moyer, *The Emerging Role of Online Communication Between Patients and Their Providers*, 19 J. GEN. INTERNAL MED. 978 (2004); Stephen E. Ross et al., *Providing a Web-Based Online Medical Record with Electronic Communication Capabilities to Patients with Congestive Heart Failure: Randomized Trial*, 6 J. MED. INTERNET RES., Apr.–June 2004, *available at* http://www.jmir.org/2004/2/e12/.

71. Alejandro (Alex) R. Jadad, *What Will It Take to Bring the Internet into the Consulting Room: We Cannot Remain Oblivious to Our Patients' Expectations*, 20 J. GEN. INTERNAL MED. 787, 787 (2005); S. H. Woolf et al., *Promoting Informed Choice: Transforming Health Care to Dispense Knowledge for Decision Making*, 143 ANNALS INTERNAL MED. 293, 295 (2005).

72. Terry, *supra* note 44, at 28–29.

73. One estimate puts these costs of repeat testing at 15% of system costs. MARKLE FOUNDATION, LINKING HEALTH CARE INFORMATION: PROPOSED METHODS FOR IMPROVING CARE AND PROTECTING PRIVACY 3 (2005), http://www.connectingforhealth.org/assets/reports/linking_report_2_2005.pdf; *see also* Michael Weiner et al., *Using Information Technology to Improve the Health Care of Older Adults*, 139 ANNALS INTERNAL MED. 430, 430 (2003).

74. Dewey Freeman, *Pay for Performance: A Win for the NHIN?*, 59 HEALTHCARE FIN. MGMT. Aug. 2005, at 120, 120; Paul C. Tang & W. Ed. Hammond, Commentary, *A Progress Report on Computer-Based Patient Records in the United States*, *in* THE COMPUTER-BASED PATIENT RECORD: AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE (Richard S. Dick et al. eds., 1997).

Large-scale third-party payers currently use electronic data sets to compare local variations in utilization and quality of care,[75] a trend that can only be expected to continue.

Third, the growth of "shared care," whereby the patient shares responsibility with the care provider and is likely to have increasingly episodic relationships with multiple providers, requires patients to have access to health data generally and, more controversially, to information in their health records.[76] Furthermore, "shared care" requires that providers have transparent access to other occasions of treatment received by the patient, particularly pharmacotherapy.[77] Thus, "shared care" used in home care settings—among providers or between providers and family members or other means of support—may also benefit from access to electronic records.[78]

Finally, healthcare consumers and regulators are demanding increasing amounts of data regarding medical errors, quality of care, and treatment outcomes.[79] This information is difficult to generate without sophisticated data coding and nearly impossible to analyze without complex database systems. The Health Plan Employer Data and Information Set (HEDIS) measures,[80] for example, are more accurate if they are based on chart reviews rather than billing records, but it is expensive and cumbersome to examine paper charts.[81] With electronic records, it is far simpler to get an accurate picture of the extent to which providers are meeting performance indicators.

Beyond improved coordination of patient care and outcomes measurement, electronic record data sets may serve critical public health goals. The Centers for Disease Control and Prevention have noted the likely usefulness of such records in monitoring immunization rates and

75. *See* Leonard D. Schaeffer & Dana E. McMurtry, *Perspective: Variation in Medical Care: Time for Action*, HEALTH AFF. (Nov. 16, 2005), http://content.healthaffairs.org/cgi/content/abstract/hlthaff.w5.552v1 (follow link to PDF or HTML version of article).

76. *See, e.g.*, Jem Rashbass, Student JAMA, *The Patient-Owned, Population-Based Electronic Medical Record: A Revolutionary Resource for Clinical Medicine*, 285 JAMA 1769 (2001); Christopher C. Tsai & Justin Starren, Student JAMA, *Patient Participation in Electronic Medical Records*, 285 JAMA 1765 (2001).

77. *See, e.g.*, TREENA A. CHOMIK, PROVINCIAL HEALTH SERVICES AUTHORITY, A REPORT ON SHARED CARE 40–41 (2005), *available at* http://www.phsa.ca/NR/rdonleyres/76D687CF_6596_46FE_AA9A_A536D61FB038/12130/SharedCareReportAug2005.pdf (listing pharmacotherapy as part of a system guideline that would "facilitate the implementation of shared care").

78. Maria Hagglund et al., *Integration Architecture of a Mobile Virtual Health Record for Shared Home Care*, 116 STUD. HEALTH TECH. INFORMATICS 340, 340–41 (2005).

79. *See, e.g.*, Laura Landro, *Consumers Need Health-Care Data*, WALL ST. J., Jan. 29, 2004, at D3.

80. "HEDIS is a set of standardized performance measures designed to ensure that purchasers and consumers have the information they need to reliably compare the performance of managed health care plans." National Committee for Quality Assistance, The Health Plan Employer Data and Information Set (HEDIS) (2006), http://www.ncqa.org/Programs/HEDIS.

81. Developed by the National Committee for Quality Assurance, HEDIS measures are standard comparisons of the performance of managed care plans. *See id.*

supporting efforts to contain outbreaks.[82] Electronic records can generate and automatically transmit state-mandated reports such as diagnoses of infectious diseases or prescriptions of controlled substances. They may also help in detecting patterns of disease outbreaks.[83] Related arguments have been made in the wake of Hurricane Katrina that EHRs are necessary to better facilitate disaster relief.[84] If EHR architecture is designed to facilitate anonymized data sets, these goals can be furthered consistently with the privacy, confidentiality, and security protections we defend in this article.

B. Patient Concerns and Perceptions

Patients cite privacy, together with security, as their issues of greatest concern about electronic records.[85] The International Medical Informatics Association lists patient privacy (and confidentiality) as a core ethical principle: "All persons have a fundamental right to privacy, and hence to control over the collection, storage, access, use, communication, manipulation and disposition of data about themselves."[86] Data from several recent surveys indicate that privacy protection remains highly salient for patients—and that this salience may be even greater among patients with diagnoses of illness and among racial and ethnic minorities. According to a 2005 survey conducted by the California HealthCare Foundation, 67% of Americans are concerned about the privacy of their health records.[87] An even greater percentage (73%) of ethnic and racial minority patients in the survey expressed concern about the privacy of health information.[88] One in eight respondents reported having engaged

82. *See, e.g.*, Ctrs. for Disease Control & Prevention, *Immunization Information System Progress—United States 2003*, 54 MORBIDITY & MORTALITY WKLY. REP. 722, 723 (2005); John W. Loonsk, *BioSense—a National Initiative for Early Detection and Quantification of Public Health Emergencies*, 53 MORBIDITY MORTALITY WKLY REP. Supp. 53, 55 (2004); John W. Loonsk et al., *The Public Health Information Network (PHIN) Preparedness Initiative*, 13 J. AM. MED. INFORMATICS ASS'N 1, 1 (2006).

83. *See, e.g.*, B. C. H. Ang et al., *An Assessment of Electronically Captured Data in the Patient Care Enhancement System (PACES) for Syndromic Surveillance*, 34 ANN. ACAD. MED. SINGAPORE 539, 540 (2005); Roger S. Magnusson, *Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System*, 24 SYDNEY L. REV. 5, 38–42 (2002).

84. Bob Brewin, *Leavitt: Katrina Demonstrates Need for e-Health Records*, GOV'T HEALTH IT, Sept. 8, 2005, *available at* http://www.govhealthit.com/article90691-09-08-05-Web ("If there was ever a case for [EHRs], this disaster underscores the need." (quoting Mike Leavitt, Sec'y, Dep't of Health & Human Servs.)).

85. *E.g.*, Laura Zurita & Christian Nohr, *Patient Opinion—EHR Assessment from the Users Perspective*, 11 MEDINFO 1333 (2004).

86. Eike-Henner W. Kluge, *Security and Privacy of EHR Systems—Ethical, Social, and Legal Requirements*, 96 STUD. HEALTH TECH. INFORMATICS 121, 122 (2003); Int'l Med. Informatics Ass'n, IMIA Code of Ethics for Health Information Professionals (2002), *available at* http://www.imia.org/English_code_of_ethics.html (adopted Oct. 4, 2002).

87. CAL. HEALTH CARE FOUND., NATIONAL CONSUMER HEALTH PRIVACY SURVEY 2005, EXECUTIVE SUMMARY 1 (2005), *available at* http://www.chcf.org/documents/ihealth/ConsumerPrivacy2005ExecSum.pdf.

88. *Id.*

in actions to protect their privacy that might have compromised their healthcare, including avoiding seeing a physician, asking a physician to fudge a diagnosis, paying to keep information out of insurance records, or avoiding medical testing altogether.[89] These behaviors were more frequent among patients with chronic diagnoses, such as cancer or diabetes.[90] Over half of the respondents surveyed indicated concerns about whether providing health information might compromise their employment or job opportunities.[91] This report concludes that protection of data confidentiality and security are critically important if patients are to trust electronic records systems.[92]

Another recent survey from a group at Johns Hopkins, designed to test whether special privacy concerns attached to genetic information, generated similar findings.[93] Patients with several different diagnoses, together with a control group of well patients, were surveyed about their preferences regarding keeping their health information private.[94] The survey results indicated that patients with genetic diagnoses were no more inclined to keep information private than patients with other diagnoses, but revealing genetic diagnoses did appear to put patients at greater employment risk than revealing other diagnoses.[95] The data did indicate, however, that the extent to which people call themselves "private" about their health conditions varies with gender (males more), race (African Americans more), and disease condition.[96] Not unexpectedly, patients with HIV were more concerned to keep their diagnosis private—but so were patients with colon cancer, a finding that suggests that the information patients consider private may not be limited to psychiatric and sexual matters.[97]

Still other data from the Hopkins group indicate that many patients would prefer not to have their medical records used in research, without separate consent.[98] This study attempted to assess the acceptability to

89. *See also* PEW INTERNET & AM. LIFE PROJECT, EXPOSED ONLINE: WHY THE NEW FEDERAL HEALTH PRIVACY REGULATION DOESN'T OFFER MUCH PROTECTION TO INTERNET USERS (2001), *available at* http://www.pewinternet.org/pdfs/PIP_HPP_HealthPriv_report.pdf.

90. CAL. HEALTH CARE FOUND., *supra* note 87.

91. *Id.*

92. The patient search for privacy is not limited to concerns about technology. *See e.g.*, *Single Hospital Rooms Rekindle Debate*, BUS. FIRST OF BUFFALO, Feb. 5, 2006, http://www.bizjournals.com/buffalo/stories/2006/02/06/story1.html (detailing conversion of semiprivate into single rooms in New York in response to patient demands for increased privacy).

93. Nancy E. Kass et al., *Medical Privacy and the Disclosure of Personal Medical Information: The Beliefs and Experiences of Those with Genetic and Other Clinical Conditions*, 128A AM. J. MED. GENETICS 261 (2004).

94. *Id.* at 262.

95. *Id.*

96. *Id.* at 262.

97. *Id.* at 264.

98. Nancy E. Kass et al., *The Use of Medical Records in Research: What Do Patients Want?*, 31 J.L. MED. & ETHICS 429, 430 (2003).

patients of HIPAA's[99] standards for waiver of consent for the use of medical records in research: that the research is no more than minimal risk, that it could not be conducted without the waiver, and that it has been reviewed and approved by an IRB.[100] Previous reported studies appear schizophrenic: in one study, only 18% found the use of medical records in research fully acceptable, and 34% of patients found the use completely unacceptable; but other studies found that, when actually asked, overwhelming majorities of patients tended to give consent.[101]

The Hopkins group surveyed patients with a variety of disease diagnoses, many who had been involved in research studies at Hopkins. They found 31% willing to allow the use of their records in research if it would improve medical knowledge, but over half unwilling to allow the use of their records without consent.[102] A large majority (86%) of those surveyed, however, would be willing to allow anonymous use of their records without consent.[103] The Hopkins group concluded that patients should be enlisted as partners in the research enterprise, with more full discussion about the use of records and efforts to obtain consent in advance, even in quite general terms, for future record use.[104]

Finally, a 2006 survey by Harris Interactive found that 68% of respondents thought that electronic medical records would improve quality of care by reducing the number of redundant or unnecessary tests, 60% thought that EMRs would reduce healthcare costs, and 55% thought that they would reduce medical errors.[105] However, 62% of respondents considered that the use of EMRs would make it more difficult to guarantee patient privacy.[106]

C. Autonomy vs. Instrumentalism

The accepted rationale for health privacy and confidentiality is autonomy.[107] A patient exercises his autonomy-based right of privacy when he shares (or declines to share) information with his healthcare provider or, for that matter, with anyone else. Any subsequent disclosure by the provider is policed by autonomy-based confidentiality. Constitutional and common law confidentiality protections suggested a

99. Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 U.S.C., 42 U.S.C., 26 U.S.C.).

100. 45 C.F.R. § 164.512(i) (2005).

101. Kass et al., *supra* note 98, at 429–30. These studies indicated that willingness to give consent varied with treatment condition; patients being seen for mental healthcare, eye care, trauma, or gynecology care were less likely to give consent.

102. *Id.* at 431.

103. *Id.*

104. *Id.* at 433.

105. Wall Street Journal Online/Harris Interactive Health-Care Poll, *supra* note 3.

106. *Id.*

107. TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 410 (4th ed. 1994).

rights-based approach[108] to legal confidentiality that paralleled the autonomy principle. In contrast, the modern law of medical confidence (particularly the federal code) does not appear to be based on an autonomy model but on a more limited instrumental model.

The simplest (and least corrosive) instrumental justification for medical confidentiality is that patients provide information to physicians to further their diagnosis with the correlate that physicians respect confidences in order to encourage patients to disclose personal and medical information that will make diagnosis and treatment more effective. This instrumental approach becomes dangerous when applied to institutional or industrial models of care. In such models, the notion too easily falls prey to arguments that see the generation, dispersal, and processing of longitudinal patient health information primarily as a necessity to reduce overall healthcare costs and to minimize medical error. As the context changes, therefore, the simple and innocuous instrumental approach becomes increasingly problematic.[109]

This movement to an instrumental rationale for protecting patient information was exacerbated by HIPAA. Congress adopted what was promulgated as the HIPAA-EDI[110] model of health transactions to reduce the "back-end," transactional costs of healthcare delivery.[111] The concomitant HIPAA federal confidentiality code[112] was enacted to minimize objections to and maximize participation in a transactional model desired by industry and promoted by government. As chillingly confirmed by the Third Circuit Court of Appeals in *Citizens for Health v. Leavitt*,[113] the federal standards have gutted the nascent rights-based ap-

108. *See, e.g.*, Humphers v. First Interstate Bank of Or., 684 P.2d 581, 587 (Or. Ct. App. 1984), *aff'd in part*, *rev'd in part*, 696 P.2d 527 (Or. 1985).

> [T]here is widespread public knowledge of the ethical standards of the medical profession and widespread belief that confidences made by a patient to a physician may not be disclosed without the permission of the patient. Patients . . . have the right to rely on this common understanding of the ethical requirements which have been placed on the medical profession and to obtain damages against a physician if he violates such confidentiality.

Id.; *see also* Duquette v. Superior Court *ex. rel.* County of Maricopa, 778 P.2d 634, 640 (Ariz. Ct. App. 1989) ("[T]he public has a widespread belief that information given to a physician in confidence will not be disclosed to third parties absent legal compulsion, and we further believe that the public has a right to have this expectation realized.").

109. *See generally* Nicolas P. Terry, *What's Wrong with Health Privacy?*, *in* THE LAW AND BIOETHICS (Ana Smith Iltis & Sandra H. Johnson eds., forthcoming 2007).

110. Wikipedia offers this definition of EDI:

> Electronic Data Interchange (EDI) is the computer-to-computer exchange of structured information, by agreed message standards, from one computer application to another by electronic means and with a minimum of human intervention. In common usage, EDI is understood to mean specific interchange methods agreed upon by national or international standards bodies for the transfer of business transaction data, with one typical application being the automated purchase of goods and services.

Wikipedia, *Electronic Data Interchange*, http://en.wikipedia.org/wiki/Electronic_Data_Interchange (last visited Oct. 3, 2006).

111. *See* Marie C. Pollio, *The Inadequacy of HIPAA's Privacy Rule: The Plain Language Notice of Privacy Practices and Patient Understanding*, 60 N.Y.U. ANN. SURV. AM. L. 579, 585–86 (2004).

112. 45 C.F.R. §§ 160, 164 (2005).

113. 428 F.3d 167 (3d Cir. 2005); *see infra* text accompanying note 209.

proach to privacy and confidentiality, preferring an instrumental rationale that is almost totally focused on institutions and compliance.

This process is being endorsed during the adoption of EHR technologies. Process-driven, technologically enabled healthcare delivery, of which the EHR is a core component, seeks to minimize the role of the individual autonomous physician (and the correlative autonomous patient). These next-generation healthcare technologies replace autonomy and choice with systems that identify while simultaneously commodifying patients (e.g., by positively identifying them with bar codes) and reduce discretion in treatment (e.g., by relying on Clinical Practice Guidelines and Clinical Decision Support Systems). Such technologies have a huge, potentially deleterious impact on individuals' privacy and confidentiality. "Yet, they are likely to be accompanied by minimalist protections that, as with the federal standards in HIPAA, will be designed so as not to impede the overall error-reduction model, for example, by favoring outcomes research to further the greater good of population-based care."[114] As we argue in this article, the adoption of EHR technologies should be used as an opportunity to reverse this trend and adopt an approach to patient privacy and confidentiality that recognizes an autonomy-based, default position of full patient control over personal information.[115] This default should be compromised only in a narrow range of circumstances, such as allowing the information to flow within the "circle of care" or medical teams, to be shared after real and informed consent by the patient, or to be used in cases where the data has been fully stripped of identifiers. An initial clarification, however, should be emphasized at this point: our claims in what follows apply only to EHRs; nothing we say is intended to apply to or to preclude current practices in which patients consent to the sharing of their health information. Our point is only that these processes should continue to take place outside of the development of the EHR architecture, at least in its initial trial period.

D. Promoting Privacy, Confidentiality, and Security

EHRs are not like paper records writ larger. The differences for patient privacy and confidentiality and data security are matters of kind, not simply matters of degree. The irony is that the more inefficient a health records system, the more it is silo-based and makes interoperability difficult, the fewer confidentiality and security issues it will pose.[116] However, such inefficient systems will not realize the potential benefits of an EIHR. Multisite EMRs or EHRs raise the stakes for protection of important values for patients: patient privacy, informed consent about

114. Terry, *supra* note 109.

115. *See generally* Cass R. Sunstein, *Privacy and Medicine: A Comment*, 30 J. LEGAL STUD. 709, 711–12 (2001).

116. *See generally* Hodge et al., *supra* note 5.

what will be included in records and with whom these records will be shared, and accuracy of records and resulting quality of care. The basic issues here are accessibility, security, and replicability. Electronic records can be viewed from across the globe; cut, pasted, or otherwise altered; and copied and recopied with a switch of the finger.[117] All occur apparently invisibly, though means of tracking changes are of course possible.

The prevailing article of faith espoused by policymakers and regulators in the United States is that patient information (be it transactional or safety related) is to be protected by mechanisms to ensure data confidentiality and security.[118] Confidentiality (mislabeled by HIPAA as "privacy") limits access to previously disclosed patient data, thus denying the option to leverage data for secondary uses such as marketing or patient profiling. Security keeps out "hackers" who would misappropriate, damage, or destroy data. In this article, we challenge the effectiveness of this protective model in the EIHR context and defend the importance of both limiting data access to providers within the "circle of care" on a need-to-know basis, and basing the choice of which EHR architecture to implement on the need to maximize data security.

Patient privacy refers to the extent to which information about patients is gleaned in the first place. A decision by a patient not to share information with a provider, or to give misleading information, both exercises and protects privacy, but at the sacrifice of timely, accurate diagnosis and treatment. Efforts by patients to obtain healthcare services without having them entered into their medical records—such as anonymous HIV testing—also protect privacy, but at the cost of what may be important omissions in the medical record that can adversely affect patient care.

The principal patient privacy question posed by EHRs is whether patient information should be entered into a system of electronic records in the first place. As an interoperable electronic record system is developed, there are a number of options for protecting patient privacy. Patients could enter an interoperable system only on an "opt-in" basis; otherwise, their records would remain silo-ed in the offices of providers. Or, patients could be allowed to specify that records from particular providers or from particular visits be omitted from the electronic record. Still another option would allow patients to specify that certain types of sensitive information be kept out of the electronic record.

Patients who do not opt in to a linked records system will lose whatever benefits might attend an interoperable system. Some of the benefits of electronic records, such as the use of clinical decision support tools that can be downloaded to an office computer or automatic generation of

117. *See* PEW INTERNET & AM. LIFE PROJECT, *supra* note 89, at 3.
118. *See, e.g.*, MARKLE FOUNDATION, *supra* note 73, at 43–58.

reminders and other informational letters to patients, are available with electronic records that are fully isolated from linkages beyond the individual provider's office. Other benefits, however—including the use of internet-based provider-patient communication systems; off-site access to records; coordination of records among providers; or inclusion of records in larger data sets designed to monitor care quality, patient safety, or patient outcomes—are available only in limited forms or are completely unavailable with fully silo-ed records. It can be expected that, as use of electronic records grows, this option will become increasingly difficult to maintain.

A second privacy-protective option would allow patients to specify that entire records from particular providers, or entire records of particular visits, be kept out of any linked electronic record system. Patients might want, for example, to exclude from the electronic record visits to any mental health professionals, treatment for sexual dysfunction, or the fact that an HIV test was performed. Patients may also wish to exclude information gathered in visits for second opinions; they may wish to be able to reconfirm or reevaluate diagnoses or treatment recommendations without informing their original care provider of additional consultation. Exclusion of such records, however, may compromise the accuracy of the electronic record; providers accessing the record may assume that it is complete and, relying on it, make decisions about care based on records that omit critical information. Such omissions can be dangerous; diagnosis and treatment may fail to take account of the use of psychotropic medications or drugs for erectile dysfunction, for example. Providers might remain suspicious of records' inclusiveness—or records might even be flagged for incompleteness—but as electronic records increasingly become the standard of care, reliance on them is likely to become routine.

Despite these difficulties, in order to maintain trust in an electronic record system it may be important to require informed consent on an individual provider basis before patient records are entered into a linked system. A report from the Markle Foundation concludes that this guarantee is necessary to generate trust in linked records systems.[119] The report recommends that current providers not enter records into a linked system without consent and that consent be negotiated for the entry of prior records.[120] The Markle report also recommends that anonymous or pseudonymous record entry be explored where linked data sets are necessary for outcomes research or public health surveillance.[121]

Yet another privacy-protective option would allow patients to stipulate exclusion of certain types of information from the medical record:

119. *See* MARKLE FOUNDATION, *supra* note 73, at 31–32.
120. *See id.*
121. *Id.* at 32.

information about genetic testing,[122] HIV testing, or treatment for conditions such as sexually transmitted diseases, for example. This option also raises difficulties about the integrity of the record for treatment purposes. In addition, it may be costly and impractical, depending on system design. Any system that requires physicians (or office staff) to redact embargoed information from the medical record before it is entered into the linked electronic record will require time-consuming processes of data separation as well as a two-tier medical record system. Primary providers will need to remember to consult the complete record; secondary providers will not know what has been omitted from the linked record. Moreover, it may prove impossible to effectively segregate all of the embargoed information; information left in the linked record may be as revealing of the patient's condition as redacted information. For example, redaction of an HIV test may not protect the privacy of a patient who does not want information about a diagnosis of HIV/AIDS in the medical record, if the record also contains a note about treatment for an HIV-related fungal infection.

Electronic record design that separates data fields at the time of record creation may be less costly to administer. Yet such "pull" systems are flawed because they are limited by the information the patient chooses to include, but may not effectively cull out all the information the patient wishes to exclude. A "pull" system that enters all prescription data, for example, may be as revealing of a diagnosis of HIV/AIDS as the actual HIV test itself.

Patients are justly concerned about what an EIHR may mean for their privacy. On the other hand, records system designs that attempt to protect privacy by choosing the information entered into the record in the first place are potentially both misleading and difficult to maintain. At present, therefore, it seems that the best way to protect patient privacy is to provide for patients to join an EIHR on an opt-in basis, rather than being entered into such a system automatically. If larger data sets are needed for outcomes research or for disease surveillance, they could be constructed with anonymous or with pseudonymous records. Complete records would be entered into the system for patients who opt in.

As a national EIHR is developed, safeguards also will need to be put into place to protect patient confidentiality; downstream limitations on the disclosure of patient information should be included in the EIHR. The most protective standards would ensure that health records are not shared without patient consent except within the "circle of care"—that is, with practitioners who are immediately and directly involved in the care of the patient—and on an as-needed basis with another member of a patient's medical team. This assurance is one of the most important guarantees for patients. Given patient attitudes towards the privacy of their

122. *See generally* David E. Winickoff, Isaac S. Kohane & Russ B. Altman, *Health-Information Altruists*, 354 NEW ENG. J. MED. 530, 530–31 (2006).

healthcare information, suspicion of electronic records, and the disadvantages detailed above of protecting patients by excluding information from the record, these confidentiality guarantees are essential.

Just as with paper records, there will be situations in which electronic health information cannot be kept confidential. The format of the record will not change state reporting requirements for conditions as varied as gunshot wounds, abuse, infectious diseases, or factors that impair driving capacity. Providers should discuss limits on confidentiality with patients before giving care, as providers ideally do now when there is a likelihood of required reporting. What may be changed are the ease, speed, and certainty of reporting. Record architecture could be designed so that providers enter data only once, but that reportable data is transferred automatically as it is entered into the record, without implicating other information in the record. For example, some states require reporting of controlled substance prescriptions to state agencies; providers then search the database before prescribing controlled substances to guard against drug abuse or diversion.[123] This entire process can be electronic. In advance of receiving such prescriptions, patients can be informed both of the requirement that the medications be entered into databases and of their providers' protocols for searching databases. Patients who do not want their information entered into the database could reject the prescription. The ease and speed of electronic transmissions intensify the importance of informing the patient when reporting is anticipated. A similar structure of single entry/copied data could be utilized when patients consent to the sharing of particular information outside of the circle of care, such as for billing purposes. Our point here is not to reject current structures by which patients consent to sharing healthcare information; it is that such means for sharing should be built in at the point of data entry, not at the point of the full EHR.

Serious questions of accuracy and fraud attend any electronic records system. EHRs can be erased, cut, or pasted without the kind of physical trail left when offices are broken into and paper records are tampered with. EHRs are also searchable, and such searches are quick and cheap. This raises the stakes about what is included in a record. A note or an unauthorized alteration, dating from many years in the past, can be brought back to notice more quickly than in a paper record. With paper, it is far more likely that old or inaccurate records will simply remain buried and unremarked; unearthing the records would take a long read through the paper file and might be regarded as irrelevant. To be sure, paper records can also be altered. But conventions have been developed to guard against such malfeasance: records must be dated, en-

123. *See, e.g.*, Office of Health Professionals Regulation, Board of Pharmacy: Controlled Substance Reporting Update, http://www.health.ri.gov/hsr/professions/csr_reporting.php (last visited Oct. 3, 2006); Utah Dep't of Commerce, Utah's Controlled Substance Database, http://csdb.utah.gov/ (last visited Feb. 1, 2007).

tered in ink, etc. Erasures can be apparent visually. With electronic records, similar conventions must be developed to ensure data integrity and facilitate audit.[124]

Data integrity will require a method for authentication. With electronic records, there must be a method in place to ensure that entries are dated and signed. Unique identifiers that are difficult to steal will be needed to authorize entries, and penalties should attach to unauthorized sharing of identifiers. Methods will also need to be implemented to track and prevent any entry changes. Records should be correctable, but there should be a method of noting that a correction has been made and what the correction entailed. Otherwise, the integrity of all electronic records will be suspect. Still another difficulty is the need to guard against careless copying of records and the possibility that errors will be introduced thereby. The Veterans Health Administration has found that one in ten electronic records contains plagiarized text and has implemented detection software as a result.[125] Conventions for data entry and authentication need to be commonly used and understood among all providers.

One of the most difficult issues for data security is to ensure that records are not subject to inappropriate access that is either inadvertent or deliberate.[126] In order to gain access to paper records, someone must be physically present with the record. By contrast, inadvertent release of records and computer hacking are notorious problems with certain electronic records—credit card information, for example.[127] Courts have wrestled with the risks of identity theft raised by electronic records such as financial statements involved in divorce proceedings; they have responded with solutions such as keeping the records in encrypted PDF files on silo-ed local networks without outside access.[128] Medical information is at least as sensitive as information of these kinds, and before it is assembled in a linkable, accessible fashion, these issues of protection

124. For a criticism of the data integrity and security mechanisms in Australia's HealthConnect record system, see Livia Iacovino, *Trustworthy Shared Electronic Health Records: Recordkeeping Requirements and HealthConnect*, 12 J.L. & MED. 40 (2004).

125. Kenric W. Hammond et al., *Are Electronic Medical Records Trustworthy? Observations on Copying, Pasting and Duplication*, AM. MED. INFORMATICS ASS'N ANN. SYMP. PROC. 269 (2003).

126. *See, e.g.*, Dan Richman, *Hacker at UW Medicine Revealed*, SEATTLE POST-INTELLIGENCER, Feb. 16, 2006, *available at* http://seattlepi.nwsource.com/local/259725_computer16.html (disclosing that hacker had opportunity to access two million patient records for eighteen months before security hole discovered); Jaikumar Viyayan, *FBI Probes Hacking Incident at Indiana Clinic*, COMPUTERWORLD, Feb. 10, 2006, http://www.computerworld.com/securitytopics/security/story/0,10801,108585,00.html.

127. For a discussion of technical issues in data security, see Mike Boniface & Paul Wilkin, *ARTEMIS: Towards a Secure Interoperability Infrastructure for Healthcare Information Systems*, 112 STUD. HEALTH TECH. & INFORMATICS 181 (2005).

128. For discussions of the difficulties courts have faced in implementing electronic records systems, see, for example, Peter A. Winn, *Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information*, 79 WASH. L. REV. 307 (2004); Kristen M. Blankley, Note, *Are Public Records Too Public? Why Personally Identifying Information Should Be Removed from Both Online and Print Versions of Court Documents*, 65 OHIO ST. L.J. 413 (2004). In the view of one court, paper records languished in "practical obscurity," an unlikely fate for electronic records. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989).

must be solved.[129] Records of any unauthorized access must be kept, and patients must be assured that they will be notified if their records have become subject to unauthorized examination.[130] Such record-keeping and notification systems can be inexpensive if the default mechanism is an e-mail to the patient of an unauthorized record access, combined with general publicity about large-scale breaches of data security.[131]

Another difficult issue with electronic records is the ease with which they can be duplicated and multiplied. Of course, paper records can be copied too. But with electronic records, multiple copies can be generated at the flick of a key, more readily than the brooms in *The Sorcerer's Apprentice*. These copies can materialize as e-mail attachments, burned CDs, easily transported diskettes or portable hardware devices, among other forms. As with paper records, copies of EHRs should not be made or shared without patient permission, except as within ordinary provider office practice. Electronic safeguards should be in place to detect when copying has taken place.

Once "out," electronic copies of an electronic record cannot be easily traced or retrieved. Indeed, it may not be clear where all the copies have gone. Information that should not have been included in the record, that was inaccurate and has been corrected in the record by the original provider, or that was inappropriately linked, may never be corrected in copies that have been released. The analogous problem arises for copies of paper records that were made at a given point in time, but it is exacerbated with the ease of transmission of electronic records. In addition to the risks of confidentiality, this ease of transmission poses real risks for the care of mobile patients; if the "wrong" electronic record is accessed, patient injury may be the result.

Finally, methods must be developed for tracking what is done with electronic records that have been properly released and for redacting information that should not have been released. For example, providers sometimes include information in records that is not medically related, such as social security numbers. This type of information should not be released in the first place, but if it is, it should be subject to tracing and redaction. Information in a record is sometimes corrected or updated, and there must be ways to ensure that these additions are made to records that were previously released. If updated information, such as a diagnostic test that reveals a prior false positive, is not included in all copies, this omission creates the risk that accuracy will be falsely assumed and that care will be directed inappropriately.

129. *See generally* Joseph Menn, *ID Theft Infects Medical Records*, L.A. TIMES, Sept. 25, 2006, at A1 (describing the consequences of and difficulties in preventing medical identity theft).

130. Ethan Preston and Paul Turner note that disclosure regimes are required in California and in the European Union. Ethan Preston & Paul Turner, *The Global Rise of a Duty to Disclose Information Security Breaches*, 22 J. MARSHALL J. COMPUTER & INFO. L. 457 (2004).

131. This is the default regime in California. CAL. CIV. CODE § 1798.82(g)(3) (West Supp. 2006).

These concerns about privacy, data confidentiality, and data security place special pressures on the creation, maintenance, and use of electronic records. They raise difficulties that must be solved before linkable, searchable, and accessible electronic records are generalized to the population. Many of these issues raise complex technical questions. Others require the development of practices such as informed consent before identifiable information about patients is entered into databases or linked with other records. We return to these issues in the discussion of strategies for record development, patient choice, and regulation below.

IV. THE LEGAL LANDSCAPE

As already noted, the Bush administration has framed the privacy-confidentiality "issue" as one involving state laws whose divergence creates a barrier to the successful implementation of a national EIHR.[132] The apparent conclusion is that the HIPAA Privacy of Individually Identifiable Health Information (PIHI)[133] savings clause for more stringent state laws[134] should be rescinded.[135] In contrast, we argue that the issue should be framed as how to resolve the serious privacy-confidentiality issues raised by a national EIHR system.[136] Part of that analysis depends on an examination of the extent to which patient privacy-confidentiality under such a system would be protected by existing legal controls.

A fundamental terminological problem obscures comprehension of the current state of the protection of health information in the United States. The media, commentators, courts, and legislators frequently refer to health "privacy" issues or protective models. In fact, two distinct issues must be addressed, issues that find articulation in two separate legal doctrines. Personal health information may be under threat either by its collection or its disclosure. The law has responded to those threats sepa-

132. *See supra* note 4 and accompanying text.

133. *See* OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (2003), *available at* http://www.hhs.gov/ocr/combinedregtext.pdf.

134. 45 C.F.R. § 160.202 (2005).

135. *See, e.g.*, Health Information Technology Promotion Act of 2006, H.R. 4157, 109th Cong. § 205 (2006) (contemplating national uniform standards on confidentiality and security and with preemptive effect).

136. *See also* Letter from Consumer Coalition for Health Privacy (CCHP) to Scott Wallace, Chairman, Comm'n on Systemic Interoperability (Oct. 7, 2005), *available at* http://www.healthprivacy.org/usr_doc/Commission_Letter.pdf. In this letter, the CCHP

> strongly urge[s Chairman Wallace] to abandon any recommendation that takes privacy rights away from patients. In fact, instead of disabling protections, there should be a serious effort to bolster and extend established privacy rights. While the HIPAA Privacy Rule serves as a solid foundation for protecting privacy, it does not address many of the issues health information technology raises. For instance, many entities collecting and sharing electronic health information are not covered by the law. In this context, stripping consumers of current safeguards is not just misguided but dangerous, and would undoubtedly have a drastic impact on the extent to which patients are willing to engage in health information technology initiatives.

Id.

rately, expressed as the distinct models of *privacy* and *confidentiality*.[137] A privacy model places limitations on data *collection*.[138] Such a model could, for example, prohibit all collection in certain circumstances or limit collection via a proportionality rule (e.g., only information necessary for treatment). The confidentiality model places limitations on data *disclosure* (e.g., hospital records may be disclosed to physicians, but not drug companies). Related protective models are either ancillary or corollary. For example, a right of anonymity provides the patient with a method to ensure privacy,[139] while security systems create the technical environment to limit access to information to those records subject to confidentiality-based disclosure control.

Although frequently described in terms of privacy and privacy law, the legal protections applied to patient health information by the common law, state statutes, or the HIPAA federal standards have very little to do with either. As will be seen, the law of privacy (or collection-centric legal models) is narrowly circumscribed and underdeveloped. In contrast, the confidentiality protective model, whereby limitations are placed on data *disclosure*, is well established in U.S. law.[140]

Contemporary U.S. confidentiality and privacy models (particularly as applied to an EIHR) are shaped and constrained by several persistent features. First, the regulation of medical records is primarily a creature of state law.[141] Second, the law relating to the privacy of medical information is woefully underdeveloped.[142] Third, while comparatively mature, state common law and statutory medical confidentiality regulations provide few solutions to the threats posed by an EIHR.[143] Fourth, the more recent HIPAA Privacy Regulations[144] have created a (frequently parallel) federal *confidentiality* code whose flaws become considerably more obvious when mapped to an EIHR. Finally, U.S. law generally permits patients to waive or sign away almost all controls on the collection or dissemination of their personal health information.[145] In only very limited circumstances are there bright-line rules rendering health information inalienable.[146]

137. *Health Record Hearings*, *supra* note 6, at 5.
138. *Id.*
139. *See infra* text accompanying notes 239–44.
140. *See* Hodge et al., *supra* note 5, at 1468 (1999).
141. *See id.*
142. *See id.* at 1467.
143. *See id.* at 1468.
144. Security and Privacy, 45 C.F.R. § 164 (2005).
145. *See, e.g.*, 45 C.F.R. § 164.503.
146. *See* Hodge et al., *supra* note 5, at 1468.

A. State Law Paradigms

Historically, the governance of medical records has been a matter of state law.[147] As a result, ownership of records, access to records, mandatory reporting, and data protection rules vary by state. The HIPAA transactional standards represent one very important exception to this general rule, but an incomplete and flawed exception because the so-called privacy provisions (but not the security or transactional rules) are subject to a savings clause preserving some state protections.[148] State-centricity is inconsistent with the proposed U.S. EIHR system. Whether truly national or regionally based, the EIHR will be an interstate creature. And, for the promise of the EIHR to be fulfilled, data must be entered only one time and must be accessible from any part of the country.

It is generally accepted that doctors own the medical records they keep about patients.[149] State statutes have extended that default position to hospital records.[150] In addition to federal regulatory[151] and Joint Commission on Accreditation of Healthcare Organizations (JCAHO) accreditation rules,[152] state law (state statutory, licensing, or even common law malpractice requirements) imposes duties of accuracy, completeness, legibility, and timeliness.[153] State statutes may prohibit the alteration of records,[154] while diverse common law remedies for spoliation create disincentives to their concealment or destruction.[155] Although

147. *See id.*

148. 42 U.S.C. § 1320d-2 (2000); *see also* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, Sec. 264(c)(2) (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.).

149. *See, e.g.*, American Medical Association, E-7.04 Sale of a Medical Practice, http://www.ama-assn.org/ama/pub/category/8381.html (last visited Oct. 3, 2006); *see also* Breen v. Williams (1996) 186 C.L.R. 71 (Austl.); Regensdorfer v. Orange Reg'l Med. Ctr., 799 N.Y.S.2d 571 (2005) (dealing with ownership, transfer, and lending of mammography and pathology films).

150. *See, e.g.*, TENN. CODE ANN. § 68-11-304(a)(1) (1995) ("Hospital records are and shall remain the property of the various hospitals . . . .").

151. Medicare Conditions of Participation: Medical Record Services, 42 C.F.R. § 482.24(b)(c) (1999).

152. "The medical record contains sufficient information to identify the patient; support the diagnosis/condition; justify the care, treatment, and services; document the course and results of care, treatment, and services; and promote continuity of care among providers." 2005 CRITICAL ACCESS HOSPITAL STANDARDS: MANAGEMENT OF INFORMATION IM.6.10.6, at 14 (Joint Commission on Accreditation of Healthcare Organizations ed., 2005).

153. *See, e.g.*, N.M. STAT. § 61-6-15 D (1978) ("'Unprofessional or dishonorable conduct' . . . includes . . . (33) improper management of medical records, including failure to maintain timely, accurate, legible and complete medical records"); NEV. REV. STAT. § 630.3062(1) (2003); WYO. STAT. ANN. § 33-26-402(a) (xxvii) (G) (2005); Nieves v. Chassin, 625 N.Y.S.2d 344. (N.Y. App. Div. 3d 1995); Schwarz v. Bd. of Regents, 453 N.Y.S.2d 836, 836–37 (N.Y. App. Div. 3d 1982); *see also* Thomas v. United States, 660 F. Supp. 216, 218. (D.D.C. 1987) (keeping inadequate summary records may constitute malpractice).

154. *See, e.g.*, NEV. REV. STAT. ANN. § 630.3062-2.

155. *See, e.g.*, Rosenblit v. Zimmerman, 766 A.2d 749, 754–58 (N.J. 2001) (canvassing various remedies and adopting independent tort remedy); *cf.* Brown v. Hamid, 856 S.W.2d 51, 57 (Mo. 1993) ("The Missouri cases, statutes, and common law address a physician's duty to let the patient inspect and copy medical records. They do not create an independent duty to *maintain* medical records. To be sure, in another case, failure to maintain medical records may contribute to, or constitute, medical

supplemented by Federal Medicare rules,[156] state statutory rules generally continue to govern records retention.[157]

B. Privacy

Although the U.S. Constitution does not contain any generalized right of privacy, the Supreme Court has recognized limited privacy rights derived from various constitutional provisions.[158] *Whalen v. Roe* is the foundational case, recognizing not only autonomy or decisional privacy ("independence in making certain kinds of important decisions"),[159] but also informational privacy ("the individual interest in avoiding disclosure of personal matters").[160] *Whalen* concerned the validity of a state statute requiring computerized record keeping (including patient identification) of scheduled prescription drugs. The Court held that, on the record as presented, arguments of potential breach of security or confidentiality by IT, medical, or judicial actors did not "pose a sufficiently grievous threat to either interest to establish a constitutional violation."[161]

The *Whalen* court recognized "a host of . . . unpleasant invasions of privacy that are associated with many facets of health care," while noting that such disclosures "are often an essential part of modern medical practice."[162] Although *Whalen* did not decide the issue,[163] the court hinted that such an invasion would rise to the level of a constitutional violation only if such a scheme failed to "evidence a proper concern with, and protection of, the individual's interest in privacy."[164]

Since *Whalen*, several federal courts have recognized constitutionally protected privacy rights in connection with medical[165] and prescrip-

malpractice. . . . There is no need, in this case, to recognize an independent tort of negligent maintenance of medical records.").

156. *See, e.g.*, 42 C.F.R. § 482.24(b)(1) (2005) ("Medical records must be retained in their original or legally reproduced form for a period of at least 5 years.").

157. *See, e.g.*, LA. REV. STAT. ANN. § 40:2144(F) (2001 & Supp. 2006); N.M. Stat. Ann. § 14-6-2 (LexisNexis 2003).

158. *See* Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965). *See generally* Roe v. Wade, 410 U.S. 113, 152 (1973) ("[A] right of personal privacy, or a guarantee of certain areas or zones of privacy" is rooted in "the First Amendment; in the Fourth and Fifth Amendments; in the penumbras of the Bill of Rights; in the Ninth Amendment; or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment." (citations omitted)).

159. Whalen v. Roe, 429 U.S. 589, 599–600 (1977).

160. *Id.* at 599.

161. *Id.* at 600–02.

162. *Id.* at 602.

163. "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." *Id.* at 605–06.

164. *Id.*

165. *See, e.g.*, Herring v. Keenan, 218 F.3d 1171, 1175 (10th Cir. 2000); F.E.R. v. Valdez, 58 F.3d 1530, 1535 (10th Cir. 1995); Lankford v. City of Hobart, 27 F.3d 477, 479 (10th Cir. 1994); A.L.A. v. W. Valley City, 26 F.3d 989, 990 (10th Cir. 1994); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 580 (3d Cir. 1980).

tion records.[166] Although recognized, this informational privacy right is not absolute. For example, in *Douglas v. Dobbs*,[167] a recent Tenth Circuit case stemming from a court-authorized police search of pharmacy records, the court noted: "We have no difficulty concluding that protection of a right to privacy in a person's prescription drug records . . . is sufficiently similar to other areas already protected within the ambit of privacy."[168] However, this abstract right was insufficient given that the plaintiff failed her burden of showing that the right has been violated by the defendant of record.[169]

Several state constitutions explicitly protect privacy.[170] Typically this privacy right has been applied to medical records. For example, one state high court opined: "Because Georgia recognizes an even broader concept of privacy [than the federal constitution], the personal medical records of this state's citizens clearly are protected by that right as guaranteed by our constitution."[171] However, as with its recognition by the federal courts, this right of informational privacy is not absolute and is subject to typical public health, law enforcement, and other exceptions.[172]

At common law, it is beyond cavil that, as one court has stated, "[i]f there is any right of privacy at all, it should include the right to obtain medical treatment at home or in a hospital for an individual personal condition (at least if it is not contagious or dangerous to others) without personal publicity."[173] Such a broad statement notwithstanding, U.S. privacy law limitations on data collection in the healthcare domain are less than robust. The Restatement's black-letter law of "privacy"[174] fails to provide any general or comprehensive "right of privacy." Rather, the "right" is a bundle of discrete tort actions and is highly qualified at that.[175] The patient must rely on factually restricted,[176] doctrinally lim-

166. *See, e.g.*, United States v. Sutherland, 143 F. Supp. 2d 609, 610 (W.D. Va. 2001).

167. Douglas v. Dobbs, 419 F.3d 1097 (10th Cir. 2005).

168. *Id.* at 1102.

169. *Id.* at 1103. The defendant in this § 1983 action was an assistant district attorney who had approved a police officer's decision to request authorization from the court to conduct a warrantless investigation of pharmacy records.

170. *See, e.g.*, ALASKA CONST. art. I, § 22; FLA. CONST. art. I, § 23; GA. CONST. art. I, § 1, ¶ 1.

171. King v. State, 535 S.E.2d 492, 494 (Ga. 2000).

172. *See, e.g.*, Limbaugh v. State, 887 So. 2d 387 (Fla. Dist. Ct. App. 4th Dist. 2004); Frank v. State, 912 So. 2d 329 (Fla. Dist. Ct. App. 5th Dist. 2005); Rollins v. Ulmer, 15 P.3d 749, 750 (Alaska 2001).

173. Barber v. Time, Inc., 159 S.W.2d 291, 295 (Mo. 1942).

174. RESTATEMENT (SECOND) OF TORTS § 652 (1965); *see also* Afro-Am. Publ'g Co. v. Jaffe, 366 F.2d 649, 653 (D.C. Cir. 1966) (recognizing common law tort); Reid v. Pierce County, 961 P.2d 333 (Wash. 1998) (adopting § 652).

175. *See, e.g.*, Gilbert v. Med. Econ. Co., 665 F.2d 305, 310 (10th Cir. 1981) (outlining incidents of malpractice by doctor and including her psychiatric history was protected First Amendment). For further discussion of privacy rights, see Lee v. Calhoun, 948 F.2d 1162 (10th Cir. 1991), where a doctor publicly defended himself against a high profile malpractice claim by arguing in a newspaper that the misdiagnosis occurred because the patient had not disclosed that he had AIDS. *Id.* at 1164. The court dismissed the subsequent invasion of privacy claim by the patient on the basis that the patient had become a public figure and malpractice was a matter of public interest. *Id.* at 1165.

ited,[177] and somewhat clumsy protections against "unreasonable intrusion upon the seclusion of another"[178] or "public disclosure of private facts."[179] As a result, common law privacy actions tend to be successful in only a few extreme or outlying cases of medical intrusions[180] or publications.[181]

C. Confidentiality

Prior to the promulgation of the federal standards, most states had developed robust common law and statutory protections applicable to the confidentiality of health information. For example, there is now considerable consistency across the states in recognizing an "independent" or torts-based remedy for breach of confidence.[182] The cause of action is theoretically (and variously) based on licensing statutes, the physician's evidentiary privilege, common law principles of trust, the Hippocratic oath, and general principles of medical ethics.[183] Only a handful of states reject the general proposition,[184] although some persist in grounding it on an outmoded doctrinal basis such as implied contract or breach of a fiduciary relationship.[185]

The common law action for breach of confidence differs from the less-developed common law tort of privacy. One court has stated the most practical difference: "Only one who holds information in confi-

176. *See, e.g.*, Knight v. Penobscot Bay Med. Ctr., 420 A.2d 915 (Me. 1980) (finding no evidence that a hospital worker's husband who observed a stranger's labor and delivery had intended the intrusion); Corcoran v. Sw. Bell Tel. Co., 572 S.W.2d 212 (Mo. Ct. App. 1978) (requiring that defendant intended or permitted unreasonable publication); Fisher v. State, 106 P.3d 836 (Wash. Ct. App. 2005) (requiring deliberate intrusion); *see also* Mikel v. Abrams, 541 F. Supp. 591, 597, *aff'd* 716 F.2d 907 (8th Cir. 1983) (breach of privacy not applicable to doctor's disclosure to plaintiff's spouse); Tooley v. Provident Life & Accident Ins. Co., 154 So. 2d 617 (La. Ct. App. 1963); Curry v. Corn, 277 N.Y.S.2d 470 (N.Y. Special Term 1966); *cf.* Colleen M. v. Fertility & Surgical Assocs. of Thousand Oaks, 34 Cal. Rptr. 3d 439 (Cal. Ct. App. 2005) (patient had reasonable expectation of privacy that clinic would not disclose specific nature of her treatment to ex-fiancé, notwithstanding her charging of treatment on his credit card).

177. *See, e.g.*, Tureen v. Equifax, 571 F.2d 411, 419 (8th Cir. 1978) (requiring "disclosure to the general public or likely to reach the general public"); *see also* RESTATEMENT (SECOND) OF TORTS § 652D cmt. c. (1977) (discussing "highly offensive" requirement).

178. RESTATEMENT (SECOND) OF TORTS § 652(A)(2)(a) (1977).

179. PROSSER AND KEETON ON TORTS 856 (W. Page Keeton et al. eds., 5th ed. 1984).

180. *See, e.g.*, Estate of Berthiaume v. Pratt, 365 A.2d 792 (Me. 1976) (physician intruded into a dying cancer patient's "physical or mental solitude or seclusion" when he took unauthorized photographs); *see also* Swarthout v. Mut. Serv. Life Ins., 632 N.W.2d 741 (Minn. Ct. App. 2001) (doctrine applicable when a life insurance company altered an applicant's medical information release, used it to obtain information from other sources, and transmitted the information to a medical records database, which was available to other insurers).

181. *See, e.g.*, Vassiliades v. Garfinckel's, 492 A.2d 580, 585 (D.C. 1985) (upholding verdicts of invasion of privacy based on publicity of private facts and breach of fiduciary duty against plastic surgeon for use of "before" and "after" photographs of patient).

182. *See, e.g.*, *id.* at 592; Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999); McCormick v. England, 494 S.E.2d 431 (S.C. Ct. App. 1997). *See generally* Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426 (1982).

183. *See, e.g.*, *Vassiliades*, 492 A.2d at 590.

184. *See, e.g.*, Quarles v. Sutherland, 389 S.W.2d 249, 252 (Tenn. 1965).

185. *See, e.g.*, Fierstein v. DePaul Health Ctr., 24 S.W.3d 220, 223 (Mo. Ct. App. 2000).

dence can be charged with a breach of confidence. If an act qualifies as a tortious invasion of privacy, it theoretically could be committed by anyone."[186] The converse is also true: if information that is not secret or private is entrusted in confidence, its subsequent disclosure may be actionable.[187]

Many states now also have some form of legislation that protects medical information against disclosure, though few contain a comprehensive prohibition against the disclosure of confidential medical information. Rather, and similar to the HIPAA code, state statutes tend to create a provider "disclosure" code detailing the large number of "safe harbor" occasions and circumstances in which healthcare and other actors are permitted to disclose confidential medical information.[188] Also, like HIPAA, the legislation in most states does not permit a private right of action by patients.[189] Some state laws protect only health information in the hands of the state, not in the offices of private providers.[190]

Both federal[191] and state courts[192] have denied any implied private cause of action for HIPAA breaches. As a result, the importance of the common law action for breach of confidence and similar causes of action[193] remains, notwithstanding HIPAA, unless and until the federal government legislatively preempts all "more stringent" state laws.

D. Limitations of HIPAA "Privacy"

The HIPAA federal standards apply to a broad range of "covered entities"[194] that transmit health information in electronic form, but by no means to all entities that maintain health information in electronic form.

186. Humphers v. First Interstate Bank, 696 P.2d 527, 530 (Or. 1985).

187. *See id.* at 528–29.

188. *See, e.g.*, Colleen M. v. Fertility & Surgical Assocs. of Thousand Oaks, 34 Cal. Rptr. 3d 439, 443 (Cal. Ct. App. 2005) (applying California statute's general and specific disclosure exceptions). See also the savings provisions in Missouri's S.B. No. 1041, 93d General Assemb. (Mo. 2006) (2006) (otherwise criminalizing "knowingly obtaining, receiving, or selling personal health information without consent").

189. *Cf.* WASH. REV. CODE ANN. § 70.02.170 (West 2002).

190. Hodge et al., *supra* note 5, at 1468.

191. *See, e.g.*, Poli v. Mountain Valleys Health Ctrs., Inc., No. 2:05-2015-GEB-KJM, 2006 WL 83378, at *3 (E.D. Cal. Jan. 11, 2006); Univ. of Colo. Hosp. v. Denver Publ'g Co., 340 F. Supp. 2d 1142, 1144–45 (D. Colo. 2004); O'Donnell v. Blue Cross Blue Shield of Wyo., 173 F. Supp. 2d 1176, 1180 (D. Wyo. 2001).

192. *See, e.g.*, Cmty. Hosp. Group, Inc. v. Blume Goldfaden Berkowitz Donnelly Fried & Forte, P.C., 885 A.2d 18 (N.J. Super. Ct. App. Div. 2005), *modified on other grounds*, 894 A.2d 702 (N.J. Super. Ct. App. Div. 2006).

193. *See, e.g.*, Doe v. Smith, 913 So. 2d 140, 143 (La. Ct. App. 2005) (finding patient stated claim for negligence when medical center violated state law by leaving patient records in parking lot where they could have been copied or disseminated); Foster *ex rel.* J.L. v. Hillcrest Baptist Med. Ctr., No. 10-02-143-CV, 2004 WL 254713, at *3 (Tex. App. Feb. 11, 2004) (holding negligence action could be brought against hospital for failure to exercise reasonable care in formulation of confidentiality policies); *see also Poli*, 2006 WL 83378, at *3 (denying motion to dismiss a negligence claim based on the release of medical information).

194. 45 C.F.R. § 160.103 (2005).

These providers,[195] such as hospitals, physicians, and health plans, are subject to the regulations if they transmit health information "in electronic form in connection with a [HIPAA-EDI transaction]."[196] The federal standards place limitations on the disclosure of "protected health information,"[197] including information that "relates to the past, present, or future physical or mental health or condition of an individual"[198] and identifies or could identify the individual.[199] Thereafter, the provider may disclose private health information (PHI) only as permitted by the federal standards.[200] Modeled as they are on existing state statutory protections, the HIPAA standards do not protect health privacy. The standards are in essence a federal *confidentiality* code based around a regulatory compliance model rather than one that creates patient rights.[201] HIPAA's principal achievements are to require that the entities it covers give patients notice of "privacy practices"[202] and protect EHRs from access outside of the entity without patient consent.[203] Privacy notices and patient consent are relatively pro forma, in the views of some critics.[204] Although HIPAA has made it less likely that, for example, employers will access employee health records from insurance claims, it contains limited safeguards. For example, covered entities are not required to inform patients about unauthorized access to their records, although entities are required to provide an accounting of such access upon request.[205]

Unfortunately the federal standards are flawed and, as currently written, will do little to create patient trust or physician participation in an EIHR. In the words of one editorial: "With an Orwellian turn of phrase, the 'privacy rule' has little to do with patient confidentiality. In fact, it permits the widespread sharing of medical data among 800,000 or so health, business and government entities."[206] First, the standards con-

195. Defined in 45 C.F.R. § 160.103.

196. 45 C.F.R. § 160.102.

197. *Id.* § 160.103.

198. *Id. But see* Rogers v. NYU Hosp. Ctr., 795 N.Y.S.2d 438, 441 (Sup. Ct. 2005) (disclosing identity of patient's roommate in general rehabilitation where hospital would not disclose roommate's medical condition).

199. 45 C.F.R. § 160.103.

200. *Id.* § 164.502(a).

201. "[The legislation] does not focus on individuals whose privacy may be at risk, but instead on regulating persons who might have access to individuals' health information." Univ. of Colo. Hosp. Auth. v. Denver Publ'g Co., 340 F. Supp. 2d 1142, 1145 (D. Colo. 2004); *see also* Logan v. Dep't of Veterans Affairs, 357 F. Supp. 2d 149, 155 (D.D.C. 2004).

202. 45 C.F.R. § 164.520.

203. 45 C.F.R. § 164.306 (requiring protection of the confidentiality, integrity, and availability of all protected electronic health information). For a discussion of what HIPAA does and does not accomplish, see Mark Rothstein, *Currents in Contemporary Ethics: Research Privacy Under HIPAA and the Common Rule*, 33 J.L. MED. & ETHICS 154 (2005).

204. *E.g.*, Pollio, *supra* note 111; Mitchelle C. Pierre, Note: *New Technology, Old Issues: The All-Digital Hospital and Medical Information Privacy*, 56 RUTGERS L. REV. 541 (2004).

205. 45 C.F.R. § 164.528.

206. *A Dose of Bad Medicine*, PHILA. INQUIRER, Jan. 6, 2006, at A16; *see also* Theo Francis, *Taking Control: Setting the Records Straight; When you sign medical-privacy forms, what exactly are you agreeing to? Probably not what you think*, WALL ST. J. (Eastern edition), Oct. 21, 2006, at R4.

centrate almost exclusively on the *process* of patient consent to disclosure. A true privacy-confidentiality regime should be more *substantively* concerned with limiting the collection and dissemination of personal health information. Questions of patient consent to disclosure only need to be addressed at the margins.

Second, the standards as amended by the Bush administration now lack any consent-to-disclosure provision for most healthcare activities.[207] That amendment deprived the patient of a symbolic privacy-autonomy "moment" at the commencement of the provider-patient relationship. More specifically, in the EHR context, the amended regulation removes any requirement for consent to disclosure for "routine uses": "treatment, payment, or health care operations."[208] The amendment was challenged, in *Citizens for Health v. Leavitt*, as violating constitutional rights and the enabling legislation.[209] The Third Circuit ruled that any Fifth Amendment substantive due process or First Amendment claims failed in the absence of state action.[210] Further, the court held that the amendment was not *ultra vires* the HIPAA statute because, in part, the statutory purpose was not to enhance patient privacy but to improve the efficiency of the healthcare system.[211]

Third, although HIPAA confidentiality is premised on national standards, the confusing and operationally obstructive "more stringent" partial preemption rule—the so-called HIPAA floor—undercuts this model.[212] Indeterminacy is further increased by the interplay between federal and state law regarding some "required by law" disclosures.[213] Indeed, one circuit has held that a state's more stringent medical-records privilege does not apply in federal-question actions.[214]

Fourth, the federal standards apply broad, arguably overbroad, exceptions (public health, judicial, and regulatory) where patient consent to data processing is not required.[215]

Fifth, the privacy standards are still too lax regarding secondary uses of patient information. There are still many unrestricted uses of patient information outside of treatment and billing; in too many situations

207. *See, e.g.*, 45 C.F.R. §§ 164.502, 164.506. In contrast, 45 C.F.R. § 164.506 as originally promulgated generally required consent even for these routine uses.

208. "A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations" § 164.506(b)(1).

209. 428 F.3d 167 (3d Cir. 2005).

210. *Id.* at 177–85.

211. *Id.* at 185. See the discussion of instrumentalism *supra* Part III.C.

212. 45 C.F.R. § 160.202 (2005); *see, e.g.*, United States *ex rel.* Pogue v. Diabetes Treatment Ctrs. of Am., Civ. No. 99-3298, 2004 U.S. Dist. LEXIS 21830, at *10–12 (D.D.C. May 17, 2004); Nat'l Abortion Fed'n v. Ashcroft, 03 Civ. 8695, 2004 U.S. Dist. LEXIS 4530, at *9 (S.D.N.Y. Mar. 18, 2004).

213. 45 C.F.R. 164.512 (2005); *see, e.g.*, United States v. Mathis, 377 F. Supp. 2d 640, 645 (M.D. Tenn. 2005) (Tennessee law in child abuse cases).

214. Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923, 925 (7th Cir. 2004); *see also* Kalinoski v. Evans, 377 F. Supp. 2d 136, 140–41 (D.D.C. 2005).

215. 45 C.F.R. § 164.512; *see, e.g.*, *Kalinoski*, 377 F. Supp. 2d at 139 (D.D.C. 2005).

patient consent for secondary uses is not required,[216] and in other situations consideration should have been given to prohibiting some consented-to secondary uses (e.g., the sale of patient data for pharmaceutical marketing).[217]

Sixth, because of limitations in the enabling legislation, the federal standards simply could not include all medical data or all users of such data.[218] There are gaps in the legislation caused by the "entities" or HIPAA-EDI premises that arguably deny protection to data held in some Personal or Trustee EHRs. Additionally, the "business associate" extension is a cumbersome and inefficient extension of the regulatory reach and is of dubious effectiveness as EIHR data processing is moved offshore.[219]

By way of example, consider *Beard v. City of Chicago*,[220] a relatively obscure employment discrimination case against a fire department. The plaintiff sought production of documents describing medical leaves of absences taken by similarly situated coworkers. The fire department kept a large number of medical records, which were generated by both staff physicians who determined whether employees were fit to return to duty and (with employee consent) by employees' outside treating physicians. The defendant resisted production on the basis, inter alia, that patient records were protected by the HIPAA privacy regulations. An outsider unversed in the intricacies of HIPAA could be forgiven for thinking that the federal confidentiality rules would apply to the holder of medical records generated by medical personnel (albeit perhaps subject to some litigation exception). However, the court found *three* separate reasons why HIPAA was inapplicable. First, the HIPAA regulations apply only to health plans, healthcare clearinghouses, or healthcare providers who engage in HIPAA electronic transactions.[221] The *Beard* court found no evidence that the fire department was a plan, clearinghouse, or other provider under the HIPAA definition.[222] Further, even if the department was a healthcare provider, it was not engaging in electronic transactions.[223] Second, the court found that the medical records kept by the fire department did not constitute "protected health information" because

216. *See generally* 45 C.F.R. §§ 164.508, .510, .512.

217. There is also generalized laxness as HIPAA compliance declines. *See* Nancy Ferris, *Privacy Rule Compliance Said to Be Diminishing*, GOV'T HEALTH IT, Apr. 19, 2006, *available at* http://govhealthit.com/article94120-04-19-06-Web&RSS=yes.

218. *See, e.g.*, *Mathis*, 377 F. Supp. 2d at 645 (FBI not a covered entity).

219. *See, e.g.*, S.B. 1199, 47th Leg., 2d Sess. (Ariz. 2006) (requiring consent to offshore outsourcing of health information processing). *See generally* ORG. FOR ECON. CO-OPERATION AND DEV., GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://it.ojp.gov/documents/OECD_FIPs.pdf.

220. Beard v. City of Chicago, No. 03 C 3527, 2005 U.S. Dist. LEXIS 374 (N.D. Ill. Jan. 7, 2005).

221. 45 C.F.R. § 164.104(a). For an explanation of these transactions, see Nicolas P. Terry, *An eHealth Diptych: The Impact of Privacy Regulation on Medical Error and Malpractice Litigation*, 27 AM. J. LAW & MED. 361, 365–66 (2001).

222. *Beard*, 2005 U.S. Dist. LEXIS 374, at *8 (referencing 45 C.F.R. §§ 160.103, 164.502 (2005)).

223. *Id*.

the regulations explicitly excluded "individually identifiable health information in . . . employment records held by a covered entity in its role as employer."[224] Third, the regulations specifically permit disclosure of protected health information in response to a discovery request.[225]

In conclusion, as we further consider how to build patient and physician trust in an EIHR, one overarching problem with the HIPAA standards must be addressed: the standards are fatally flawed because they lack transparency and clarity. They may be labeled (really, mislabeled) as promoting "privacy," but their sheer obliqueness detracts from any educative or principled "message." What was required of the federal standards was a more generalized statement of principle based clearly on an autonomy-focused rationale, a legal guarantee that patients have control of their health information. As follows from earlier comments, exceptions should have been more narrowly constructed and tightly controlled by concepts of proportionality and the circle of care.[226]

E. Medical Information and Inalienability

One of the most pervasive characteristics of the U.S. approach to medical confidentiality and privacy is that patients may sign away almost all extant controls on the collection or dissemination of personal health information. This was operationalized at common law through the doctrine of waiver[227] and in state medical confidentiality statutes by authorization provisions.[228] Nowhere has this tendency been more obvious than in HIPAA's Personally Identifiable Health Information (PIHI) regulation. Indeed, PIHI reads less like a list of confidentiality protections and more like a catalogue of exceptions and, specifically, process rules for authorizations to avoid confidentiality. For example, although the regulation notes that authorizations are required for certain uses or disclosures of psychotherapy notes[229] and some marketing uses,[230] the bulk of the relevant regulatory text details the process to be followed to obtain such authorization.[231]

State laws that prohibit health information use or disclosures *notwithstanding authorization* are very much the exception. However, these inalienability provisions provide an interesting model, particularly given

224. *Id.* at *8–9 (citing 45 C.F.R. § 160.103); *see also* State *ex rel.* Cincinnati Enquirer v. Daniels, 844 N.E.2d 1181 (Ohio 2006) (finding lead-risk-assessment reports maintained by health department and lead-citation notices issued to property owners of units reported to be the residence of children whose blood test results indicate elevated lead levels did not contain "protected health information").

225. *Beard*, 2005 U.S. Dist. LEXIS 374, at *9–10 (citing 45 C.F.R. § 164.512).

226. *See generally* Terry, *supra* note 109.

227. *See, e.g.*, Mull v. String, 448 So. 2d 952 (Ala. 1984); Fedell v. Wierzbieniec, 485 N.Y.S.2d 460 (N.Y. Sup. Ct. 1985).

228. *See, e.g.*, CAL. CIV. CODE § 56.11 (West 1982 & Supp. 2006).

229. 45 C.F.R. § 164.508(a)(2).

230. § 164.508(a)(3).

231. § 164.508(b)(c).

the tempting secondary uses for EIHR information. For example, along with related controls (e.g., prohibiting insurers from conditioning insurability on genetic testing[232]) most states place some limitations on the use of genetic information in the health insurance domain, while a few also extend those limitations to life and disability insurance. Thus, many states prohibit the use of individuated genetic data for nontherapeutic purposes such as determining insurability or setting premiums.[233] Relatively few states undercut this prohibition by allowing for applicant consent to its use.[234] At the federal level, a presidential executive order prohibits agencies from collecting genetic information concerning federal employees.[235] There have been a series of bills introduced in Congress to make this proscription universal.[236]

Some AIDS/HIV reporting legislation has targeted similar issues.[237] State legislatures have tried to reduce disincentives to HIV testing by guaranteeing the confidentiality of the test results.[238] For example, the Illinois statute permits test subjects to remain anonymous.[239] While the same statute allows identified subjects to execute releases allowing for disclosure,[240] its overall tenor is to considerably limit the dissemination of the results, utilizing need-to-know and limited circle of care models.[241] Finally, and perhaps of most interest for our purposes, is a recent New Hampshire law that prohibits the sale of prescription information (that contains patient or prescriber-identifiable data) "for any commercial purpose," including advertising or marketing.[242] Reportedly, the statute is being challenged on First Amendment grounds by data aggregators.[243]

V. PRIVACY AND CONFIDENTIALITY STRATEGIES

Three types of strategies are available to reduce the risks associated with EHRs: specific system architectures, requirements for patient

232. *See, e.g.*, ALA. CODE § 27-53-2(a) (LexisNexis 1998); KAN. STAT. ANN. § 40-2259(b)(1) (2000); MINN. STAT. ANN. § 72A.139(3)(1) (West 2005).

233. *See, e.g.*, ALA. CODE § 27-53-2(b); GA. CODE ANN. (2005) § 33-54-4; IND. CODE ANN. § 27-8-26-5(2)–(4) (LexisNexis 1999); KAN. STAT. ANN. § 40-2259(b)(4); MINN. STAT. ANN. § 72A.139(3)(3)(4) (West 2005); OR. REV. STAT. § 746.135(3) (2005); TEX. INS. CODE ANN. § 546.052 (Vernon 2006).

234. *See, e.g.*, MO. REV. STAT. § 375.1303-1(3)–(4) (2000).

235. Exec. Order No. 13,145, 65 Fed. Reg. 6877.1-202(c) (Feb. 8, 2000).

236. *See, e.g.*, Genetic Information Nondiscrimination Act of 2005, S. 306, 109th Cong. § 104 (2005); Genetic Privacy and Nondiscrimination Act of 2003, H.R. 3636, 108th Cong. (2003) (introduced to the House of Representatives, Nov. 21, 2003); Genetic Information Nondiscrimination Act of 2003, S. 1053, 108th Cong. (2003).

237. *See, e.g.*, CONN. GEN. STAT. § 19a-583 (2005); 410 ILL. COMP. STAT. 305/1 (2005).

238. Some public health officials argue the protections go too far. *See* Marc Santora, *Overhaul Urged for Laws on AIDS Tests and Data*, N.Y. TIMES, Feb. 2, 2006, at B1.

239. 410 ILL. COMP. STAT. 305/6.

240. *Id*. 305/9(b).

241. *See, e.g.*, 410 ILL. COMP. STAT. 305/9(c)(h).

242. N.H. REV. STAT. § 318:47-f.

243. Beth Herskovits, *Freedom of Information*, PHARMACEUTICAL EXECUTIVE, Sept. 1, 2006, *available at* http://www.pharmexec.com/pharmexec/article/articleDetail.jsp?id=369271.

choice, and legal requirements can be combined to protect patient health information and generate the trust needed for an interoperable health record system to succeed. The balance of strategies chosen will depend on the EHR system architecture that is employed. The importance of developing successful strategies for protecting privacy and confidentiality cannot be emphasized too strongly.

Although the Markle Foundation's data indicate public support for easily accessible electronic records, respondents to its 2005 survey overwhelmingly (79%) regard it as a "top" or "high" priority that their medical information be shared electronically only with their consent.[244] The vast majority of respondents (91%) want mechanisms in place to confirm the identity of anyone using the system and to guarantee against unauthorized access.[245] Reviewing who has had access to personal health information is also a core priority (81%), with respondents (68%) unwilling to give employers access to their health information.[246]

The Markle Foundation endorses seven patient and consumer principles developed by the Personal Health Technology Council:

1. Individuals should be able to access their health and medical data conveniently and affordably.

2. Individuals should be able to authorize when and with whom their health data are shared. Individuals should be able to refuse to make their health data available for sharing by opting out of nationwide information exchange.

3. Individuals should be able to designate someone else, such as a loved one, to have access to and exercise control over how their records are shared.

4. Individuals should receive easily understood information about all the ways that their health data may be used or shared.

5. Individuals should be able to review which entities have had access to their personal health data.

6. Electronic health data exchanges must protect the integrity, security, privacy, and confidentiality of an individual's information.

7. Independent bodies, accountable to the public, should oversee local and nationwide electronic health data exchanges. No single stakeholder group should dominate these oversight bodies, and

244. Press Release, Markle Foundation, Americans Support Online Personal Health Records; Patient Privacy and Control over Their Own Information Are Crucial for Acceptance (Oct. 11, 2005), *available at* http://www.markle.org/resources/press_center/press_releases/2005/press_release_10112005.php.

245. *Id.*

246. *Id.*

consumer representatives selected by their peers should participate as full voting members.[247]

The recommendations we develop below endorse and develop these principles. At the outset, however, we must address the "do nothing" strategy. This approach could be premised either on an informed healthcare skeptic's intuition that the financial and structural issues posed by EHR development are insoluble, or on the more cynical view that in a couple of years some other inexpensive-until-implemented State of the Union sound bite will replace universality of health records.[248] Such a "do-nothing" strategy, however, cannot be countenanced because of the proliferation of PHRs and the growth of hospital and systemwide EMRs.[249] The latter are not EHRs in the strictest sense but single EMRs implemented by large, often regional or national healthcare systems[250] or even for federal government employees.[251] While PHRs or systemwide EMRs may not offer the same interoperability or quite the same scale as NHIN-interlinked EHRs (and thus may be somewhat more secure), they raise identical privacy and confidentiality concerns as their EHR fellow-travelers.

A. System Architectures

Four different general types of EHR architectures are available at the present time, which we label as "Personal," "Shared," "Trustee," and "Interoperable." This final type, the Electronic Interoperable Health Record (EIHR), can be structured to operate either over a regional

247. *Id.*

248. *See, e.g.*, *Insiders Say Health Bill Unlikely to Pass This Year*, GOV'T HEALTH IT, Apr. 12, 2006, *available at* www.govhealthit.com/article94051-04-12-06-Web.

249. *See, e.g.*, In-depth Focus: Kaiser Permanence, HealthConnect, http://ckp.kp.org/kpindepth/archive/indepth_faq_all.html (explaining the EMR system installed by Kaiser Permanente and designed to integrate the records of its eight million members in nine states); *see also* Deborah Vrana, *Kaiser's Prescription for Medicine is Digital*, L.A. TIMES, May 30, 2005, at C1; R.H. Dolin et al., *Kaiser Permanente's Convergent Medical Terminology*, 11 MEDINFO 346 (2004). *See generally* George C. Halverson, *Reengineering Care with KP HealthConnect*, PERMANENTE J., Fall 2004, at 28, *available at* http://www.kpihp.org/publications/docs/cis_healthconnect.pdf. In the public sector, for example, the Department of Veterans Affairs, the country's largest integrated healthcare system with 180,000 healthcare professionals and more than five million patients, uses the systemwide VistA EMR system to share records among its facilities. *See* VETERANS HEALTH ADMIN., DEP'T OF VETERANS AFFAIRS, VISTAA MONOGRAPH 2005–2006 (2006), *available at* http://www.va.gov/vista_monograph/docs/vista_monograph2005_06.pdf. The Department of Defense plans to roll out its own Armed Forces Health Longitudinal Technology Application (AHLTA) system (formerly known as CHCS II) for all uniformed service personnel and their families by 2011. AHLTA, http://www.ha.osd.mil/AHLTA/default.cfm (last visited Oct. 15, 2006); *see also* Bob Brewin, *DOD's e-Health Record System to Be Ready in a Year*, GOV'T HEALTH IT, Jan. 30, 2006, *available at* http://govhealthit.com/article92145-01-30-06-Web.

250. The EMR and EHR terminologies blend somewhat if a system creates its systemwide "EMR" by creating interoperability between discrete EMR systems installed at different sites.

251. *See, e.g.*, Federal Family Health Information Technology Act of 2006, H.R. 4859, 109th Cong. (2006). *See generally* Stephen Barr, *Bill to Promote Electronic Health Records*, WASH. POST, Mar. 2, 2006, at D4.

health information organization (RHIO) or national health information network (NHIN). Privacy, confidentiality, and security problems increase as the interoperability of the EHR system increases, with a RHIO or NHIN system posing the most pressing issues.

1. Personal EHR Model

In a personal EHR (PHR) model, patients are the dominant managers and custodians of their electronic medical records. The record consists of information fields into which data are entered either by the patient or through data export, or managed by the patient from records maintained by the patient's physician.[252] One PHR model has patients subscribing to a web-based service that assists them in collecting data from one physician and then disseminating it to others. The "Continuity of Care" record proposed by the American Academy of Family Physicians as a standardized form of summarized electronic records would be a convenient data model.[253] With a fully personal EHR system, only the consumer can download, view, combine, or process all his records. Patients would then be able to choose which records or parts of records they would export. Exported records could be provided on a read-only basis, protecting against alteration or entry of additional material. Employers,[254] hospital systems,[255] and EMR vendors[256] are also rolling out hybrid models that enable web-based access for patients to portions of their records for personal health monitoring. Future models could mimic personal financial management software such as Intuit's *Quicken*[257] or Microsoft's *Money*.[258]

However, such individually maintained records have limited usefulness. Although these records may be a helpful source of information for

252. For a description of system architecture, see William W. Simons, Kenneth D. Mandl, & Isaac S. Kohane, *The PING Personally Controlled Electronic Medical Record System: Technical Architecture*, 12 J. AM. MED. INFORMATICS ASS'N 47 (2005).

253. American Academy of Family Physicians Center for Health Information Technology, ASTM Continuity of Care Record (CCR), http://www.centerforhit.org/x201.xml (last visited Oct. 15, 2005).

254. *See, e.g.*, Carol Korne, *Toward a Digital Health-Care Ecosystem*, WALL ST. J. (Eastern edition), Oct. 25, 2005, at B2 (discussing web-based health records system for employees of IBM); Timothy J. Mullaney, *Dell Takes Health Care Online*, BUS. WK. ONLINE, Apr. 7, 2006, http://www.businessweek.com/technology/ content/apr2006/tc20060407_825324.htm.

255. *See, e.g.*, myHealthFolders, https://myhealthfolders.com (web-based health and medical information system offered by BJC HealthCare System); *see also Hospital to Boost Branding with CD-ROMS for Patients*, PHILA. BUS. J., Mar. 28, 2006, http://www.bizjournals.com/philadelphia/stories/2006/03/27/daily12.html (discussing hospital program to distribute medical records software to patients).

256. *See, e.g.*, *Cerner Touts Diabetes Internet Program*, ASSOCIATED PRESS, Oct. 12, 2005, http://www.kansas.com/mld/kansas/news/state/12883385.htm (diabetes monitoring system).

257. Intuit recently announced plans to enter the PHR market. May Wong, *TurboTax Maker to Develop Health Care Management Software*, ASSOCIATED PRESS, Apr. 13, 2006, http://mercurynews.com/mld/mercurynews/news/local/states/california/northern_california/14328152.htm.

258. *See also* Milt Freudenheim, *WebMD Wants to Go Beyond Information*, N.Y. TIMES, Feb. 23, 2006, at C1 (describing WebMD agreements with health insurers and employers to operate web-based PHRs).

patients, they are less likely to be viewed as reliable by providers. Depending on patient choices and data sources, personal records may not always be comprehensive (longitudinal) or coded for interoperability. Personal records that use a standardized format and are drawn from standardized sources, such as the Continuity of Care Record, will be in a format that permits the greatest likelihood of interoperability.

At the same time, individually maintained electronic records have the least significant implications for privacy and security. The data in such personal records will be patient-provided and maintained, thus enabling patients to keep information they regard as private out of the medical record. Confidentiality, however, will be more difficult to protect. If patients share records with providers, and providers make copies—as surely they will do for reference and liability purposes—there will be copies passed from the patients' control. Once any part of a Personal EHR leaves a patient's control and enters the control of a physician or system, more typical privacy, confidentiality, and security issues will arise. Providing copies on a read-only basis or incorporating other means of digital rights management (DRM) protects the record from alterations or additions, but not from further scrutiny or duplication through transcription.

Such personal health records could be maintained in a location of the patient's choosing. If financial records are an apt analogy, these choices are likely to include home computers, office computers, portable hard drives, smart cards, thumb drives, or other personal information devices (PIDs). Patients will have varying skills at maintaining their records; some will keep adequate backup copies, but others will leave PIDs with the only copy of their records in taxis with the same frequency that they lose their iPods. Some will sequester records on a home computer; others will wear their records on necklace PIDs. Such variability in data availability, confidentiality, and security are in the hands of the patient, and, at least to that extent, are subject to patient choice. When data are compromised or lost, moreover, it will be on an individual patient basis; there will be no large data banks of patient information subject to hacking at a single swipe (at least for non-web-based PHRs). Because of the vagaries of patients' abilities to maintain their data, however, such personal health records will not be adequate substitutes for medical records maintained by providers or systems.

2. Shared Models

A variety of systems are available in which physicians and patients share responsibility and control over electronic records, but the records remain silo-ed. When physicians retain control over their records silos, the model is physician-centric. The silo-ed records may not be interoperable, as with either paper records or many of the individual electronic records maintained today. Collecting the silo-ed records in a common

format, such as the Continuity of Care Record or some of the systemwide formats described below, allows for easy transfer or incorporation into larger data sets. However, there is significant tension between entrenched local practices for maintaining data and the desire for interoperable formats.[259]

In consultation with patients and subject to patient consent, physicians could transmit all, parts, or summaries of such records to patients, to other physicians, or to a centralized data warehouse. The most discussed example of this type of "push" system for sharing electronic records is the Australian *HealthConnect* system discussed earlier.[260] As *HealthConnect* has been pilot tested, commentators have emphasized the importance of protecting patient confidentiality; in particular they focus on the requirement of patient consent before new information is entered and patient control of access to information that has already been entered.[261] Once data enter a centralized system, the difficulties of protecting confidentiality intensify.

3. Trustee Models

In a trustee model, patients contract with a fiduciary to maintain their health records.[262] Trustee models can be offshoots of a PHR in that the data remain in the control of the patient, who then pushes all or some of the data to a trusted third party. The patient sets the terms of the trust and instructs the trustee about the management of that information, including to whom it may be disclosed, how long it may be kept, and who may add to the record. Such a model could also be an offshoot of a shared or physician-centric architecture if the physician, in consultation with the patient, initiates the "push" directly from the record to the trustee.

A trustee model has limited privacy implications in that it is the patient who decides what data is transferred to the trustee. Confidentiality is protected by a trust agreement that governs further distribution of data, but is assured only to the extent that the trustee lives up to its fiduciary responsibilities. Trustee models increase ease of access to data for

259. John E. Mattison, Robert H. Dolin, & Diane Laberge, *Managing the Tensions Between National Standardization vs. Regional Localization of Clinical Content and Templates*, 11 MEDINFO 1081 (2004).

260. For a description of the HealthConnect system, see Gunter & Terry, *supra* note 30; Roger S. Magnusson, *Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System*, 24 SYDNEY L. REV. 5, 46–50 (2002).

261. *E.g.*, Bernadette McSherry, *Ethical Issues in HealthConnect's Shared Electronic Health Record System*, 12 J.L. MED. 60, 64 (2004); Moira Paterson, *HealthConnect and Privacy: a Policy Conundrum* 12 J.L. MED. 80, 80–81 (2004).

262. For a description of a trustee model, see Paul T. Kostyack, Note, *The Emergence of the Healthcare Information Trust*, 12 HEALTH MATRIX 393 (2002). *See also* eHealthTrust, http://www.ehealthtrust.com (last visited Oct. 10, 2006).

mobile patients, but present concomitant data security issues; trustees of large data sets may be attractive targets for hackers.[263]

Moreover, once a trustee has authorized transmittal of a patient's record, it is unclear how the dissemination of the data is controlled thereafter. One model would be for the information to flow into the receiving provider's record, posing anew the issues of protecting confidentiality and data integrity. Another model would limit any data transferred from the trustee to read-only (or some other form of DRM) such that the control of the data remains with the trustee and within the terms of the trust agreement. This model protects data integrity but risks to confidentiality remain.

Many different types of trustees are possible. The trustee could be a data warehouse or some other form of repository. Trustees could be for-profit, not-for-profit, or public entities. As the number and variety of trustees increase, so will the difficulties in protecting data security, confidentiality, and transmissibility. A single trustee model might be preferable; standards could be common across the nation and problems of protection would need to be solved only once. A single trustee could nonetheless offer different arrangements for data management and protection, depending on the patient's choice.

4. Regional or National Models

A fully longitudinal, EIHR, whether operating at a regional (RHIO) or national (NHIN) level, has both the greatest advantages for patient care and public health and the most fundamental implications for patient privacy, confidentiality, and security. Current discussions suggest that a RHIO or NHIN could utilize either a data warehouse or pointer/records locator technical model. Models may be premised on the aggregation of existing EMR silos, common data standards, and sophisticated data-mining tools that improve usability and maximize the return on investments.

These RHIO and NHIN models may have different technical security implications, but they pose virtually identical privacy and confidentiality issues. A regional organization has the advantage of potential protection and at least some standardization. But depending on how it is designed, it may not afford the full advantages of mobility. If patients see providers outside of the region, there would need to be methods for allowing both access and entry of data. Further, patients might not know which region maintained their records or if their records should move with them if they permanently relocate. If the different regional organizations had different standards, moreover, patients might be confused

263. Lest this concern seem fanciful, for a list of data breaches in 2005, affecting over fifty million Americans, see Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Oct. 10, 2006).

about which standard governed their records. If a fully interoperable system is desired, therefore, it seems that the best option is a single national system. Recently, Dr. Brailer has stated, "Being a RHIO is a journey . . . . We know it has a beginning and a middle, but we don't know what the end looks like."[264] Dr. Brailer has acknowledged that RHIOs likely will morph from being fledgling technology infrastructures into governing or advisory bodies.[265] For the federal government, therefore, it is clear that the future lies in a NHIN.

As follows from the discussion above, a national, fully interoperable architecture poses the greatest privacy, confidentiality, and security risks and suggests that the protection of personal health information will depend on patient choice and legal protections.

B. Patient Choice

Legal mechanisms such as informed consent and privacy-confidentiality that operationalize patient interaction with medical services typically provide that patients may waive autonomy-derived "rights."[266] Increasingly, however, such waivers tend to pay only lip service to the underlying autonomy. Thus, informed consent (both in law and medical practice) tends to focus on the narrow issue of "consent" rather than the disclosure of information that increases patient choice and participation.[267] Similarly, patient "consent" to information sharing is often a nonnegotiable precondition to treatment—there is no genuine choice. The challenge in the EHR setting, therefore, is to identify potential choices regarding patient participation in such a system—choices that range from opting out completely, through redacting specific data or restricting occasions of disclosure, to reviewing the data that is included in the system.

1. Opting In or Opting Out

The initial option for patient choice is whether to enter into the system in the first place. This option is most protective of patient privacy; patients may decide that they want to stay "local," with their records, electronic or paper, either under their own control or at offices of their individual providers. As an NHIN is developed, it may be preferable to employ such an "opt-in" strategy for pilot programs. A trial period of

264. *Brailer: RHIOs Will Need Makeovers*, HEALTH DATA MGMT., Feb. 2006, *available at* http://www.healthdatamanagement.com/html/news/NewsStory.cfm?articleId=12762.

265. *Id.*

266. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., OCR PRIVACY BRIEF, SUMMARY OF HIPAA PRIVACY RULE (2003), *available at* http://www/hhs./gov/ocr/privacysummary.pdf (discussing consent and privacy issues).

267. *See generally Terry*, *supra* note 109.

perhaps five years would give some sense of the issues, both anticipated and unanticipated, that could arise with a NHIN.

As the reported data about patient preferences suggest, informed consent should be required before a patient is entered into the system. This consent must include decisions about what information will be included, what access will be authorized and what will not be authorized without further consent, and what provisions will be in place to secure additional consent before data are revealed. Perhaps most importantly for patient trust in a NHIN, consent should also include basic information about how data security will be protected and what steps will be taken to inform patients if there are security breaches.

If a NHIN comes into general use, however, it may be increasingly difficult in practice for patients to opt out of the network effectively. Physicians may come to rely on access to the network for information about their patients. They may use electronic searches or algorithms in assessing patients' conditions or in determining how patients have been managed in the past. Patients who are not in the NHIN may be disadvantaged as a result and the choice to opt out will become illusory. The use of evidence-based protocols is a particular case in point; patients without electronic records might be managed far differently than patients with EHRs, and physicians might be more accustomed to using the EHR. Similarly, some physicians might rely on searches of the NHIN for data about drug allergies or drug interactions. Patients who do not have information in the NHIN may be at risk if providers become less effective at using patient-provided medical histories to guard against problematic responses to prescriptions. Opting out of the network as a method of protecting confidentiality will thus come at a price that will be unacceptably high to many. Legislation also would be required to guarantee access to care for, and eliminate discrimination against, patients who opt out.

2. Circle of Care

An alternative means to protect confidentiality is to reduce the size of the population that has access to a patient's data. Making patient safety information available to all healthcare providers that are tangentially involved in a patient's care renders the level of privacy and security accorded that data a function of the weakest link in the system. Fully interoperable data is also immeasurably more valuable for secondary uses (e.g., marketing) and is an irresistibly tempting target for commercial aggregators.[268] As it becomes more difficult for patients to opt out of inter-

268. The level of commercial aggregation of personal information was highlighted by ChoicePoint's acknowledgement that the personal financial records of more than 163,000 consumers in its database had been compromised. *See* United States v. ChoicePoint Inc., No. 1:06-CV-00198 (N.D. Ga. filed Jan. 30, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf; *Personal Information: Agencies and Resellers Vary in Providing Privacy Protections: Testimony Before the Sub-*

operable networks, therefore, informed consent and patient confidentiality become increasingly important. Recognizing these pressures, we recommend that data in the system be available only to providers within the therapeutic circle of care (those within the patient's medical team) on a need-to-know basis. This is not as radical a recommendation as it might seem; as we have emphasized earlier, it does not preclude a system design that permits the generation of anonymized data sets for quality improvement or public health purposes. Nor does it preclude architectures that permit data to be copied to different fields at the time of entry with patient consent.

3. Data Carveouts

An additional confidentiality-protective strategy would be to build a mechanism for placing certain aspects of the record in a "secure" envelope, available only with specific permission of the patient. Obvious examples of sensitive information that might be carved out and secured in this way include mental health history and sexual/reproductive history (including abortion, sexual dysfunction, pregnancy, and even birth control). But it may not be easy to anticipate what information individual people would find especially important to safeguard. The data from the group at Johns Hopkins indicate that diagnoses of colon cancer are considered more sensitive by patients than other cancer diagnoses.[269] Some people might regard treatment for acne, obesity, sleeplessness, or even conditions as common as hypertension as especially sensitive. The rule that is most protective of privacy would be to permit patients to stipulate what information should be secured, although records will be less useful if significant portions are secured and providers do not know which ones these are. Three models are available for securing some, but not all, information: a secure "envelope" model, a contextual disclosure model, and an access-edit model.

a. Secure Envelope

The envelope model assumes that the patient opts in to the system (or is given no choice), but is permitted to tag specific data as "highly

comm. on Commercial and Administrative Law and the Subcomm. on the Constitution, of the H. Comm. on the Judiciary, 109th Cong. 15 (2006) (statement of Linda D. Koontz, Director, Info. Mgmt. Issues, U.S. Gov't Accountability Office), *available at* http://www.gao.gov/new.items/d06609t.pdf ("Although the information resellers that do business with the federal agencies we reviewed have taken steps to protect privacy, these measures were not fully consistent with the Fair Information Practices. Most significantly, the first four principles, relating to *collection limitation*, *data quality*, *purpose specification*, and *use limitation*, are largely at odds with the nature of the information reseller business."); Press Release, Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm (referring to settlement); *see also* Steve Bailey, *Your Data for Sale?*, BOSTON GLOBE, Mar. 24, 2006, at C1 (detailing plans by providers to sell aggregated medical data).

269. Kass et al., *supra* note 93, at 266–67.

confidential." This data is then specially coded (e.g., with a DRM layer), and although it circulates within the EIHR, is not generally readable. The secure envelope could be opened only with a specific additional consent from the patient or in the case of a particular medical interaction. Examples of the latter might include: "To be opened if unconscious in an ER," "To be opened in an OB/GYN emergency," or "To be opened if psychotropic medications are prescribed." Research would be required to determine how the conditions "on" the envelope could be coded so that they do not defeat the exercise by hinting at the secure data contained within.

b. Contextual Disclosure

Context-specific disclosure requires the patient (likely in consultation with his provider) to create different layers of health information that are made available to the EIHR. These layers would then provide for context-specific disclosure. For example, ob/gyn-related data would only be available to ob/gyn providers. Research would be required to determine the impact of such limitations on health quality or medication safety. For example, if a patient was taking Lithium and being treated in an ER following an overdose, absent knowledge of the medication or underlying diagnosis, the patient would be at extreme risk as there is no screening test for detecting Lithium.

Patient-initiated carveouts aside, an EIHR system likely would have to be coded for some layer restrictions on data because of existing restrictions on the transparency of data involving, for example, HIV/AIDS or child abuse. At present, there are immense variations in state law restricting data transparency. These variations would need to be addressed through the development of national standards or by allowing patients both to specify states in which they are likely to receive care and to code records to meet the regulations of the most restrictive state specified.

c. Access and Edit

Envelope storage or context constraints generally are discussed in terms of restrictions placed on the data upon input. However, comparable rights could be given to patients using an Access/Edit model similar to that used by the HIPAA confidentiality standards or some state statutes. Thus, a patient could be permitted to access his record and remove or request removal of specific data, or place restrictions on its dissemination (e.g., by moving it to a secure envelope). An Access/Edit system has the difficulties of any model in which some data are unavailable to treating physicians. It has the additional disadvantage for patient care that patients may use idiosyncratic judgment in securing records, but the concomitant advantage that patients will be able to exercise individualized preferences in this regard.

4. Review and Audit

As a more powerful EIHR system is developed, problems with the integrity of records must also be addressed. Record inaccuracy or corruption can adversely affect patient care—far more so than if the inaccurate record is buried in the office of an individual provider. Data security breaches carry the potential to release an entire record, rather than whatever fragment may be located in the office of an individual provider.

As electronic records are relied on more extensively, their accuracy will be important for patient safety and quality of care. Records gathered far in the past may reappear with deleterious consequences. Patients thus should be able to review their records for accuracy to be able to ensure that old inaccuracies or errors do not recur in current approaches to care. If old paper records are transformed into electronic format, patients should be able to review what is included for accuracy and to limit linkages as appropriate. As new electronic records are created, patients should be permitted to review them for accuracy to the same extent they currently can review paper records. When patients challenge the accuracy of records, corrections should be made and noted by providers where appropriate. If, in the judgment of the provider, a correction is not appropriate, there should be a way to note in the EHR that a particular aspect of the record has been challenged by the patient for accuracy but has not been amended by the provider.

Patients should also be able to ascertain whether the patient choice model selected has been employed appropriately to protect their privacy and data confidentiality. Patients should know whether secure envelopes, context-specific disclosures, and other selective strategies have been implemented in their records.

The data about patient and consumer attitudes strongly support the importance to patients of knowing whether the security of their electronic information has been breached. Developers of electronic records must explore methods for keeping patients apprised of security breaches of their health information. HIPAA seems too weak; it requires simply that custodians of electronic health information keep records about access that patients can review on request. The difficulty is that patients may not know that their records have been accessed and thus may not request information about access. A relatively simple alternative would be to keep a flagged list of who has accessed the records at the front of the record; the list should be readily apparent to the patient or anyone else accessing the record. A more aggressive strategy would permit patients to stipulate electronic contact information that they would like to have used if there are security breaches involving their medical records. A still more aggressive—but the most protective—strategy would follow California's model for security breaches of electronic information: con-

tact is required, but public notice of a security breach will suffice when contact information is not available.[270]

C. Legal Strategies

In May 2005, responding to criticisms about its Care Records Service (CRS) system,[271] the U.K. government issued the *NHS Connecting for Health Care Record Guarantee*.[272] This EHR "bill of rights" provides that the NHS CRS system will

- allow only those involved in your care to have access to records about you from which you can be identified;
- show only those parts of your record needed for your care;
- allow only authorized people to access your records (who will need a 'smart card' as well as a password);
- allow you to control whether information in electronic records made about you by the organization providing your care can be seen elsewhere in the NHS.[273]

NHS also promised future technologies such that "if you are concerned about particular entries . . . rather than about the whole record, you will be able to ask us to keep parts of the record . . . from general view and only share them with your permission . . . ."[274] Thus, the NHS plan endorses three confidentiality-privacy strategies: the "circle of care," "opt out" and "sealed envelope," which we will return to.

We believe that patient privacy and confidentiality cannot be adequately protected in a U.S. EIHR environment without similar strategies and, inevitably given our context, federal statutory or regulatory attention. *A fortiori* we believe such legal attention will be necessary to deal with the informational dangers associated with the likely choice of a national EIHR (NHIN) system. In this Section, we outline what we believe are the four key legal protections that must be introduced: first, some types of medical data should be protected against even consented-to collection or disclosure; second, all healthcare information should reside only in the medical domain; third, as a default position healthcare information should flow only within the patient's circle of care; fourth, an independent regulatory body should be appointed that will have the power

270. *See generally* CAL. CIV. CODE § 1798.29 (West 2006).

271. *See supra* text accompanying note 41.

272. NAT'L HEALTH SERV. (U.K.), THE CARE RECORD GUARANTEE (2005), *available at* http://www.connectingforhealth.nhs.uk/all_images_and_docs/crbb/crs_guarantee_2.pdf.

273. *Id.* at 3.

274. *Id.* at 7. Notwithstanding, critics and opinion polls continue to criticize the program for its potential damaging effects on physician-patient confidentiality. *See* Sam Lister, *Medical Database Is Huge Security Risk and Freedom Threat, Say Doctors*, TIMES (London), June 30, 2005, at 24.

to review the manner in which patient information is handled by any EIHR system and resolve disputes.

1. Exclusion of Data Types and Inalienability

The legal model for privacy and confidentiality in the United States has generally endorsed the approach that any and all personal information (be it financial, medical, etc.) may be collected, processed, and disseminated with the consent or authorization of the data subject. The primary operational objection to this approach is that "consent" processes are imperfect in situations involving parties with radically different bargaining strengths or in informational asymmetry regarding the implications of any such consent or authorization. A secondary objection is that data protection is sectoral: both technical and regulatory regimes among varying types of data such as financial records, insurance records, health records, employment records, and court records. It may be very difficult for people to understand and remember the differences associated with these different regimes. Gaps in data protection may be especially apparent if data are transferred across regimes, as when health records are made available to insurers or employers.[275] A third difficulty is that most data regulation is state based,[276] with state laws applicable to medical and insurance domains varying widely; any NHIN system will transcend state boundaries and thus pose the issue of whether protection is only as strong as the weakest link.

Assuming movement towards a fully interoperable national EHR and full inclusion of patient and physician stakeholders in its development, the most important measure would be a federal statute that overrides any consent/authorization regime and guarantees that certain types of private information cannot find their way into an EIHR.

Specifically, lawmakers should place limits on the collection of certain EHR information, such as Radio Frequency Identification (RFID) tracking data outside of hospital or pharmacy premises. Similarly, inalienability rules (regardless of "consent") should be applied to the disclosure of genetic information or AIDS/HIV data outside of the medical domain.

2. Medical Domain

Because of the great power and scope of the likely information in a complete EHR on a given patient, at this time EHRs should be employed for treatment purposes only. That is, they should be accessible

275. *See, e.g.*, Rebecca L. Woodard, Note, *Is Your Medical Information Safe? A Comparison of Comprehensive and Sectoral Privacy and Security Laws*, 15 IND. INT'L & COMP. L. REV. 147 (2004).

276. The HIPAA confidentiality code "exception" proves the general rule because of its "more stringent" partial preemption rule. *See supra* text accompanying note 212.

only to patients themselves and to healthcare providers for medical management. Specifically, legislation is necessary to lock out secondary users (e.g., pharmaceutical companies, life insurers, and employers) and to prohibit the commercial aggregation of identifiable EHR-sourced data.

Other uses of the entire EHR by healthcare providers—for billing purposes, for cost management, or for evidence—should not currently be permitted. These uses are simply too risky for patients if EHRs are released on an all-or-nothing basis. EHRs should not be available for these other purposes even on a consensual basis; patients may be unaware of what is in the record and what such consent really means. The information can be acquired in other ways. For example, unlinked electronic records in individual providers' offices could be used instead—just as paper records are today. If this is regarded as impractical, an alternative would be to allow entries in specified fields—but not the entire EHR—to be released with consent from the patient or the patient's representative. Or, at the point of entry, given data could be transferred with the patient's consent—e.g., for billing purposes. To be sure, achieving this separation presents a problem of software design; as providers enter data into an EHR, there will be a need to separate data for the NHIN from data used for billing purposes. But the full power of the identifiable EHR should, as systems are developed, be restricted to the medical domain.

3. Circle of Care

As discussed above, existing U.S. confidentiality provisions do little to limit the dissemination of patient-specific health information within the health domain. That is, once the data is entered, it is freely available to healthcare providers.

The common law position was discussed by the D.C. Court of Appeals in *Suesbury v. Caceres*,[277] a case involving the alleged disclosure of a patient's HIV-positive status between doctors in the same medical office in the context of a complaint about one doctor sexually molesting the patient. The court noted that "[d]octors within the same medical office should be allowed to work together with some latitude of freedom of communication not only to treat patients, but also to respond to patient administrative requests and, as here, patient complaints."[278] Cognizant that, although the doctors shared a practice, the context of the alleged disclosure was not strictly medical, the court concluded:

> It is true that, in the case before us, the communication was not made in connection with the immediate on-going treatment of a common patient. Nonetheless, the communication was related to and arose as a consequence of such medical treatment and was

277. Suesbury v. Caceres, 840 A.2d 1285 (D.C. 2004).
278. *Id.* at 1289.

made in the course of the business of administering the mutual medical practice.[279]

The HIPAA confidentiality code applies a similar, and similarly flawed approach, providing that a "covered entity may use or disclose protected health information for treatment, payment, or health care operations,"[280] with disclosure permitted if it is for the entity's "own treatment, payment, or health care operations,"[281] the "treatment activities of a health care provider,"[282] or the "payment activities" of the recipient entity.[283] We believe that patient confidentiality would be better served if the data and its dissemination were subject to a default limitation based on necessity or proportionality. For example, a "privacy" rule could limit the collection of patient data to that required for the contemplated procedure. Equally, a "confidentiality" rule could limit the dissemination of the patient data to those providers directly involved in the patient's current treatment, restricted to the "circle of care" or within the patient's medical team.

4. Regulatory Overview and Dispute Resolution

As already noted, the federal confidentiality rule is flawed in large part because its opaque regulatory language makes it difficult for patients and providers to understand the importance of health privacy and confidentiality.[284] Worse, its enforcement is in the hands of the Office for Civil Rights, Department of Health and Human Services.[285] As a result, from a patient's perspective, enforcement is placed in the hands of an "insider" primarily interested in ensuring the efficiency of the HIPAA-EDI transactional model. From a provider's perspective, HIPAA regulation and enforcement have added yet another layer of detailed regulation of healthcare and another possibility for heavy penalties or even criminal sanctions.

In contrast, a traditional "rights" analysis would suggest that those who suffer privacy-confidentiality violations should be given private rights of action against the violators, a position refuted by HIPAA and most state medical privacy laws, yet permitted by common law actions such as breach of confidence.[286] While it should be obvious that we are

279. *Id.* In a footnote the court left itself some room for future maneuver with the comment, "We limit our holding here, however, to the facts before us, namely, a communication between two physicians working together in the same medical practice, and leave a broader analysis for another day." *Id.* at 1288 n.4.

280. 45 C.F.R. § 164.506(a) (2005).

281. *Id.* § 164.506(c)(1).

282. *Id.* § 164.506(c)(2).

283. *Id.* § 164.506(c)(3).

284. *See supra* text accompanying note 226.

285. U.S. Dep't of Health & Human Servs., Office for Civil Rights—HIPAA, http://www.hhs.gov/ocr/hipaa/ (last visited Oct. 15, 2006).

286. *See supra* text accompanying notes 189–94.

privacy advocates and view violations of privacy or confidentiality as extremely serious and potentially very harmful to patients, we do not believe that most informational transgressions rise to the level of personal injuries. Any extension of traditional private rights in this area would merely embroil privacy and confidentiality in the politics[287] and cycles of tort retrenchment associated with the "malpractice crisis."

Rather, what is required is an independent, apolitical institution that can educate both patients and providers with codes of conduct and resolve disputes in a constructive, nonlitigious way. The model described is that of a government-funded independent agency or ombudsman. Australia,[288] Canada,[289] New Zealand,[290] and the United Kingdom[291] have all adopted such regulatory review and dispute resolution models as part of their data protection regimes and most have been particularly active in the health domain. For example, the Australian Privacy Commissioner is legislatively tasked with complaint investigations and audits and publishes data protection guidelines.[292] Specifically within the health domain, the Commissioner has published the influential *Guidelines on Privacy in the Private Health Sector*,[293] which spell out in comprehensible fashion both the general principles of health privacy and seek to provide guidance for specific issues. We believe that Congress should promulgate an EHR "bill of rights" and appoint an independent Health Privacy Commissioner charged with the mandate to educate patients, providers, and regulators and equipped with the powers to mediate disputes and publish codes of conduct.

VI. CONCLUSION

In May 2005, Secretary Leavitt labeled the movement to electronic records an "economic imperative" designed to "maintain health and at

287. "Despite the health care system's acute need—indeed because of it—broad coalitions across the political spectrum are tempted to co-opt medicine to advance larger agendas about the effect of lawsuits on social stability and economic prosperity. . . . [N]o matter which camp claims victory in the overall battle, the outcome will not remedy serious deficiencies in how American law deals with medical errors." William M. Sage, *Understanding the First Malpractice Crisis of the 21st Century*, HEALTH L. HANDBOOK 28 (Alice Gosfield ed., West Group 2003).

288. Office of the Privacy Comm'r (Austl.), About the Office, http://www.privacy.gov.au/about/index.html (last visited Oct. 15, 2006).

289. Office of the Privacy Comm'r of Can., About Us, http://www.privcom.gc.ca/aboutUs/index_e.asp (last visited Jan. 8, 2007). Additionally, some Canadian provinces have their own Privacy Commissioners. For example, the Information and Privacy Commissioner for Ontario has published guidelines for using RFID tags in Ontario public libraries. ANN CAVOUKIAN, PH.D., GUIDELINES FOR USING RFID TAGS IN ONTARIO PUBLIC LIBRARIES (2004), http://www.ipc.on.ca/docs/rfid-lib.pdf. The Ontario Commissioner is also responsible for aspects of health privacy under the province's Personal Health Information Protection Act, 2004.

290. Privacy Comm'r (N.Z.), Your Privacy, http://www.privacy.org.nz/your-privacy (last visited Oct. 15, 2006).

291. U.K. Info. Comm'r's Office, http://www.ico.gov.uk/ (last visited Oct. 15, 2006).

292. Office of the Privacy Comm'r, *supra* note 288.

293. OFFICE OF THE FED. PRIVACY COMM'R (AUSTL.), GUIDELINES ON PRIVACY IN THE PRIVATE HEALTH SECTOR (2001), *available at* http://www.privacy.gov.au/publications/hg_01.html.

the same time maintain the momentum of our economy."[294] There is little doubt that a well-constructed, secure EIHR can improve the quality of our healthcare, reduce medical and medication errors, and provide a platform for patients to better understand and participate in their healthcare. However, progress towards these laudable goals has, so far, reflected institutional interests and priorities. It has been an example of "insider baseball" that has focused primarily on architecture and technical standards. The debate now must be broadened to reflect the interests and participation of patients and physicians and to incorporate a principled, autonomy-based, and comprehensible privacy-confidentiality structure for EHRs.

Prior to his resignation from ONCHIT,[295] Dr. Brailer argued for a sea change in the relationship between patients, physicians, and medical records whereby physicians will relinquish ownership of medical records and, instead, become their "stewards": "[I]n black and white, no questions asked, the data belongs to patients."[296] Or, in the President's recent words: "We're really talking about making sure each American has an electronic medical record over which he or she has got control of the privacy."[297] These strong protective concepts must be fully operationalized. A cavalier, instrumental, HIPAA-like business-as-usual approach to the privacy and confidentiality of EIHR data will not suffice. Hard choices must be made as to the architectural and patient consent models that may involve subjugating some interoperability and comprehensiveness ambitions to principled protections of patient autonomy. Equally, some simple tweaking of the HIPAA confidentiality rules is insufficient. Patient privacy and confidentiality must be more broadly protected with principled and comprehensible bright-line legislation.

294. Esther Landhuis, *Health Chief: Put Data Online*, MERCURY NEWS, May 24, 2005, http://www.mercurynews.com/mld/mercurynews/living/health/11723708.htm.

295. Nicholas Timmins, *Top U.S. Health Official Steps Down*, FIN. TIMES, Apr. 20, 2006.

296. *Andis Robeznieks Brailer: IT Can Help Reverse Culture of Errors, Inefficiencies*, MOD. PHYSICIAN, Sept. 23, 2005, http://www.modernphysician.com/news.cms?newsId=4034.

297. Press Release, White House, President Participates in Panel Discussion on Health Care Initiatives (Feb. 16, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/02/20060216-3.html.