Harvard Journal of Law & Technology
Volume 22, Number 1 Fall 2008

FINDING A CURE: THE CASE FOR REGULATION AND OVERSIGHT OF ELECTRONIC HEALTH RECORD SYSTEMS

*Sharona Hoffman & Andy Podgurski**

TABLE OF CONTENTS

---

* Professor Hoffman is Senior Associate Dean for Academic Affairs, Co-Director of Law-Medicine Center, Professor of Law, and Professor of Bioethics, Case Western Reserve University School of Law. B.A., Wellesley College; J.D., Harvard Law School; LL.M. in Health Law, University of Houston. Professor Podgurski is Associate Professor of Electrical Engineering and Computer Science, Case Western Reserve University. The authors wish to thank David Aaron, Jessica Berg, Jessie Hill, Jacqueline Lipton, Maxwell J. Mehlman, Duncan Neuhauser, and Greg Vetter for comments on previous drafts. We are also grateful for the skillful research assistance of Katy Kassimatis. Research on this paper was made possible in part by support from the U.S. National Institutes of Health through the Case Western Reserve University Center for Genetic Research Ethics and Law (NIH grant # P50 HG-003390). Professor Podgurski's research was also supported by National Science Foundation grant CCF-0702693.

I. INTRODUCTION

In the foreseeable future, it is likely that the familiar, paper-based patient medical files, contained in thick folders and stored on long shelves or in filing cabinets, will become a thing of the past. Both the federal government and health care advocates are enthusiastically promoting the adoption of health information technology ("HIT") and electronic health record ("EHR") systems[1] as means to transform and improve health care in the U.S.[2]

An editorial published in *The New York Times* in August 2007 noted that the World Health Organization, in 2000, ranked the U.S. health care system 37th out of 191 and identified our poor use of in-

1. An EHR is a record of "electronically maintained information about an individual's lifetime health status and health care, stored such that it can serve . . . multiple legitimate users." BIOMEDICAL INFORMATICS: COMPUTER APPLICATIONS IN HEALTH CARE AND BIOMEDICINE 937 (Edward H. Shortliffe & James J. Cimino eds., 3d ed., Springer 2006) (1990) [hereinafter BIOMEDICAL INFORMATICS]. EHR systems, as we are using the term, are systems that add to EHR databases information management tools including clinical alerts, reminders, decision aids, links to medical literature, and tools for data analysis, such as search engines. *See id.*

2. INST. OF MED., KEY CAPABILITIES OF AN ELECTRONIC HEALTH RECORD SYSTEM 1–2 (2003) (stating that "[t]here is a great deal of interest within both the public and private sectors in encouraging all health care providers to migrate from paper-based health records to a system that stores health information electronically and employs computer-aided decision support systems" and that the "development of an IT infrastructure has enormous potential to improve the safety, quality, and efficiency of health care in the United States"); *see also* THE LEWIN GROUP, HEALTH INFORMATION TECHNOLOGY LEADERSHIP PANEL FINAL REPORT 3 (2005) (recognizing "HIT implementation as an essential, high priority for health care").

formation technology as among the primary reasons for this "dismal" ranking.[3] The editorial decried the fact that "American primary care doctors lag years behind doctors in other advanced nations in adopting electronic medical records or prescribing medication electronically."[4] Indeed, only seventeen percent of physicians in ambulatory care settings[5] use EHR systems to any extent, and only eleven percent of hospitals have fully implemented EHR systems.[6]

Medical errors have been estimated to result in as many as 98,000 deaths each year in the U.S. and to cost as much as $29 billion.[7] Appropriate use of carefully designed EHR systems could dramatically reduce those numbers. These systems can promote efficiency, diminish costs, save time, and save lives. For example, the Palo Alto Medical Foundation learned of Merck & Co.'s recall of certain batches of hepatitis A vaccine that had lost their potency and was able, using its EHR system, to identify 17,000 patients who needed to be revaccinated.[8]

The personal experiences of an emergency room doctor at a large Texas hospital provide two more vivid illustrations of the need for HER systems.[9] In one case, a woman with a splint on her arm stated that she had a broken arm, was suffering severe discomfort, and had run out of the painkillers she was given when initially treated at another hospital. In the absence of access to the other hospital's records, the doctor ordered X-rays of her arm and neck, only to discover that she had no injury. The time and expense wasted in uncovering the woman's scheme to obtain prescription narcotics could have been avoided had the physician been able to discredit her claim through a search of electronic records. In a second instance, the doctor treated a paraplegic patient who had a urinary tract infection. Because he did

---

3. Editorial, *World's Best Medical Care?*, N.Y. TIMES, Aug. 12, 2007, at WK9. France and Italy were ranked first and second. *Id.*

4. *Id*. The editorial also argued that "despite our vaunted prowess in computers, software and the Internet, much of our health care system is still operating in the dark ages of paper records and handwritten scrawls." *Id.*

5. Ambulatory care is treatment that is given at the office of a physician or other provider. *See* STEDMAN'S MEDICAL DICTIONARY 59 (28th ed. 2005) (defining "ambulatory" as "denoting a patient who is not confined to bed or hospital as a result of disease or surgery").

6. *See* AM. HOSP. ASS'N, CONTINUED PROGRESS: HOSPITAL USE OF INFORMATION TECHNOLOGY 1 (2007), *available at* http://www.aha.org/aha/content/2007/pdf/070227-continuedprogress.pdf; Catherine M. DesRoches et al., *Electronic Health Records in Ambulatory Care — A National Survey of Physicians*, 359 NEW ENG. J. MED. 50, 54 (2008). For further discussion of how many health care providers currently use EHR systems, *see infra* notes 149–52 and accompanying text.

7. TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM 1–2 (Linda T. Kohn et al. eds., 2000).

8. Meg Walker, *Electronic Medical Records Can Cure Potential Nightmares*, SAN FRANCISCO BUS. TIMES, Mar. 29, 2002, *available at* http://sanfrancisco.bizjournals.com/sanfrancisco/stories/2002/04/01/newscolumn2.html.

9. E-mail to Sharona Hoffman, Professor of Law, Case Western Reserve University Law School (Aug. 29, 2007, 22:46:00 EDT) (on file with author).

not have access to the patient's records at other facilities, the physician did not know that the infection, caused by the patient's permanent urinary catheter, was resistant to the antibiotics that he had prescribed. The patient died of heart failure in the hospital.

Politicians and government leaders have expressed great enthusiasm for the development and implementation of EHR systems. In April 2004, President George W. Bush announced plans to ensure that most Americans' health records are computerized within ten years[10] and to create a National Health Information Network ("NHIN").[11] Numerous proposed bills have been introduced in Congress to promote HIT initiatives.[12] Executive and legislative efforts at the state level have established strategies and target dates for HIT implementation, commissions to develop recommendations for HIT use, and financial incentives for HIT adoption.[13] EHR systems also became an issue in the 2008 presidential campaign, as both Senators McCain and Obama discussed their potential benefits.[14]

However, the novel and significant risks generated by EHR systems cannot be ignored.[15] Products with poor information display and navigation can impede rather than facilitate providers' work.[16] The growing capabilities of EHR systems require increasingly complex software, which heightens the danger of software failures that may harm patients. To illustrate, one report relates that a hospital phar-

---

10. The White House, A New Generation of American Innovation, Transforming Health Care: The President's Health Information Technology Plan, http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html (last visited Dec. 19, 2008).

11. Exec. Order No. 13,335, 69 Fed. Reg. 24,059 (Apr. 27, 2004); Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 686.

12. *See infra* notes 159–61 and accompanying text.

13. National Conference of State Legislatures, Health Information Technology Financing Legislation, http://www.ncsl.org/programs/health/forum/Hitch/finance.htm (last visited Dec. 19, 2008).

14. Editorial, *The Candidates' Health Plans*, N.Y. TIMES, Oct. 28, 2008, at A30 ("Both candidates have largely accepted the prevailing expert wisdom on ways to improve quality and lower health care costs over the long run, such as relying more on electronic medical records and better management of the chronically ill.").

15. *See infra* notes 102–13 and accompanying text; INTEGRATED CTR. FOR CARE ADVANCEMENT THROUGH RESEARCH ET AL., THE RELATIONSHIP BETWEEN ELECTRONIC HEALTH RECORDS AND PATIENT SAFETY: A JOINT REPORT ON FUTURE DIRECTIONS FOR CANADA 7 (2007), *available at* http://www.infoway-inforoute.ca/Admin/Upload/Dev/Document/EHR-Patient%20Safety%20Report.pdf (asserting that there is "evidence to suggest that EHRs may facilitate medical errors and/or generate new kinds of errors").

16. *See* Pamela Hartzband & Jerome Groopman, *Off the Record — Avoiding the Pitfalls of Going Electronic*, 358 NEW ENG. J. MED. 1656, 1657 (2008) ("[I]n the new electronic sea of results, it becomes difficult to find those that are truly relevant."); Christine A. Sinsky, *e-Nirvana: Are We There Yet?*, 15 FAM. PRAC. MGMT. 6, 6 (2008), *available at* http://www.aafp.org/fpm/20080300/6enir.html (arguing that existing EHR systems have severe usability problems and provide poor support to physicians).

macy's computer program generated erroneous medication order lists, leading to the delivery of the wrong drugs to patients in many wards.[17]

Thus far, the legal literature has not assessed the need for careful regulatory oversight of EHR systems akin to that required, in principle, by the Food and Drug Administration ("FDA") for life-critical medical devices.[18] This Article begins to fill that gap. It analyzes EHR systems from both legal and technical perspectives and examines how law can serve as a tool to promote HIT. Extensive regulations already exist to govern the privacy and security of electronic health information.[19] Privacy and security, however, are only two of the concerns that merit regulatory attention. Perhaps even more important are the safety and efficacy of these life-critical systems.

The benefits of EHR systems will outweigh their risks only if these systems are developed and maintained with rigorous adherence to the best software engineering and medical informatics practices and if the various EHR systems can easily share information with each other. Regulatory intervention is needed to ensure that these goals are achieved. Once EHR systems are fully implemented, they become essential to proper patient care, and their failure is likely to endanger patient welfare.[20]

The remainder of the Article will proceed as follows: Part II provides background and analysis of EHR systems, including their benefits and risks. Part III assesses the need for regulatory oversight of EHR systems. Part IV develops detailed recommendations for the contents of a regulatory framework. These recommendations include a requirement that all health care providers use approved EHR systems and that the government provide financial assistance to support the implementation of the new systems. In addition, the proposal addresses the following: the selection of an agency to regulate EHR systems; the creation of approval and monitoring processes for EHR systems; the standardization of system features and capabilities; interoperability; and the establishment of a national research databank of de-identified[21] electronic patient records. Part V concludes.

---

17. Richard I. Cook & Michael F. O'Connor, *Thinking About Accidents and Systems*, *in* IMPROVING MEDICATION SAFETY 80–82 (Kasey Thompson & Henri R. Manasse eds., 2005) (explaining that the problem was rooted in a backup tape that was incomplete and corrupted).

18. *See infra* Part III.B.1 for discussion of FDA's regulation of medical devices.

19. *See infra* notes 119–28 and accompanying text (discussing the HIPAA Privacy and Security rules).

20. *See* Frank Richards, *Infrastructure*, *in* IMPLEMENTING AN ELECTRONIC HEALTH RECORD SYSTEM 21, 21 (James M. Walker et al. eds., 2005) [hereinafter IMPLEMENTING AN EHR SYSTEM] (explaining that "falling back on manual processes when the automated system is down is problematic at best, and, in the worst case, may compromise patient care").

21. De-identified medical records are records that do not explicitly identify individuals and cannot be used to identify individuals (e.g., through social security numbers, addresses, etc.). *See* 45 C.F.R. § 164.514(a) (2007).

II. EHR SYSTEMS: BACKGROUND AND ANALYSIS

A. What Are EHR Systems?

No universally accepted definitions have been developed for "EHRs" or "EHR systems."[22] There is, however, some agreement about their essential components.[23] EHR systems, as the term is used in this Article and by other commentators, do much more than keep records.[24] In 2003, the Institute of Medicine ("IOM") identified the following elements as "core EHR functionalities":

- *Health information and data*: The system should display laboratory test results, allergies, lists of other medications the patient is taking, medical and nursing diagnoses, patient demographics, and providers' notes.[25]
- *Results management*: EHRs should provide laboratory test results, radiology procedure results, and other treatment results electronically to enhance provider access to needed information and promote efficiency and easier detection of abnormalities.[26]
- *Order entry and management*: Computerized medication orders and other care instructions can reduce or eliminate lost orders, duplicate orders, mistakes caused by illegible handwriting, and delays in filling orders.[27]
- *Decision support*: Computer reminders and prompts can improve preventive care, diagnosis, treatment, and disease management.[28]
- *Electronic communication and connectivity*: EHR systems should facilitate online communication among medical team members, other providers such as laboratories or pharmacies, and patients through e-mail, web messaging, integrated health records within and across treatment settings, telemedicine,[29]

22. *See* Ashish K. Jha et al., *How Common Are Electronic Health Records in the United States? A Summary of the Evidence*, 25 HEALTH AFF. w496, w497 (2006); *see also* ROBERT WOOD JOHNSON FOUND. ET AL., HEALTH INFORMATION TECHNOLOGY IN THE UNITED STATES: THE INFORMATION BASE FOR PROGRESS 8 (2006), *available at* http://www.rwjf.org/files/publications/other/EHRReport0609.pdf (noting the "need to develop a common, valid definition of an EHR").

23. Jha et al., *supra* note 22, at w497.

24. *See* BIOMEDICAL INFORMATICS, *supra* note 1, at 937 (noting that EHR systems include "information management tools that provide clinical alerts and reminders, linkages with external health knowledge sources, and tools for data analysis").

25. INST. OF MED., *supra* note 2, at 7.

26. *Id.* at 7–8.

27. *Id.* at 8.

28. *Id.* at 8–9.

29. Telemedicine is "the delivery of health care at a distance, increasingly but not exclusively by means of the Internet." BIOMEDICAL INFORMATICS, *supra* note 1, at 991.

> and home telemonitoring.[30] Communication should be possible among providers in different geographic locations and medical organizations.[31]

With these features, EHR systems can significantly improve medical treatment by ensuring that patients' health information is easily available to providers who require it, by preventing or correcting clinicians' errors or oversights before they cause harm, and by helping to promulgate best medical practices. In addition, EHR systems can serve important administrative functions:

- *Patient support*: Patient education and self-testing at home should be facilitated by electronic systems.[32]
- *Administrative processes*: Electronic scheduling systems, insurance eligibility verification, billing, and claims processing systems should be components of EHRs. Computerized tools can also be used to identify individuals who are potentially eligible for clinical trials, those who should be informed about a drug recall, or candidates for chronic disease management programs.[33]
- *Reporting and population health management*: Through the implementation of standardized terminology and machine-readable records, EHR systems should enable providers to collect clinical data in order to meet public and private reporting requirements.[34]

The federal government's ultimate goal is a fully interoperable EHR system. The system will initially operate on a regional basis using Regional Health Information Organizations ("RHIOs") and eventually transition to an NHIN.[35] "Interoperability" means "the ability for systems to exchange data and to operate in a coordinated, seamless manner."[36] If EHR systems across the country are made interoperable, patients who relocate to different cities or seek second opinions from doctors outside their physician networks could have their records elec-

---

30. Home telemonitoring can be defined as "an automated process for the transmission of data on a patient's health status from home to the . . . health care setting." Guy Paré et al., *Systematic Review of Home Telemonitoring for Chronic Diseases: The Evidence Base*, 14 J. AM. MED. INFORMATICS ASS'N 269, 270 (2007).

31. INST. OF MED., *supra* note 2, at 9–10.

32. *Id.* at 10.

33. *Id.*

34. *Id.* at 10–11.

35. Jeff Day, *Regional EHR Exchanges to Lead U.S. Drive, Some Say; Others See Questionable Future*, 15 BNA'S HEALTH CARE POL'Y REP. 1011, 1011 (2007); Terry & Francis, *supra* note 11, at 686.

36. BIOMEDICAL INFORMATICS, *supra* note 1, at 952.

tronically transmitted to the new physicians, who could use them on their own EHR systems.

One well known RHIO is the Regenstrief Medical Record System, which is used by numerous facilities in the Indianapolis area.[37] The system captures medical data, includes an order entry mechanism, provides reminders and informational feedback, and features search and retrieval capabilities for research purposes.[38] The largest EHR system in the U.S. is the Veterans Health Information Systems and Technology Architecture ("VistA") developed by the Department of Veterans' Affairs ("VA"). A primary component of VistA is a physician interface called the Computerized Patient Record System ("CPRS").[39] The CPRS, which has been widely praised,[40] provides complete EHRs, an order entry system, critical alerts, remote access to health information at other VA facilities, and decision support, including reminders.[41]

Some current HIT initiatives utilize two alternatives to comprehensive EHRs: continuity of care records ("CCRs") and personal health records ("PHRs").[42] CCRs are summaries that aggregate data from a variety of sources to form a limited record of the patient's provider and insurance information, current health care status, and medical history, including allergies, medications, diagnoses, and recent procedures.[43] These subsets of full patient EHRs can be e-mailed to the patient's next care giver or given to the patient on paper or portable electronic media to be taken to her next appointment.[44] While useful, CCRs are not as comprehensive as full EHRs, and, unlike EHR systems, CCR systems do not offer order entry mechanisms,

37. *See* Clement J. McDonald et al., *The Regenstrief Medical Record System: A Quarter Century Experience*, 54 INT'L J. MED. INFORMATICS 225, 226–28 (1999).

38. *Id.* at 225–27, 248.

39. *See* Jonathan B. Perlin et al., *The Veterans Health Administration: Quality, Value, Accountability, and Information as Transforming Strategies for Patient-Centered Care*, 10 AM. J. MANAGED CARE 828, 828, 832 (2004). *See generally* DEP'T OF VETERANS AFFAIRS, COMPUTERIZED PATIENT RECORD SYSTEM (CPRS) USER GUIDE (2008) (on file with the author) [hereinafter CPRS USER GUIDE] (describing the VA's CPRS and its features).

40. *See, e.g.*, Joel Kupersmith et al., *Advancing Evidence-Based Care for Diabetes: Lessons from the Veterans Health Administration*, 26 HEALTH AFF. w156, w156 (2007) (stating that the VA's Veterans Health Administration provides "a unique laboratory for using the [EHR] to transform health care and accelerate discovery"); Perlin et al., *supra* note 39, at 832.

41. Perlin et al., *supra* note 39, at 832–33.

42. Terry & Francis, *supra* note 11, at 687–88.

43. CTR. FOR HEALTH INFO. TECH., ESSENTIAL SIMILARITIES AND DIFFERENCES BETWEEN THE HL7 CDA/CRS AND ASTM CCR 1–2 (2005), *available at* http://www.centerforhit.org/PreBuilt/chit_ccrhl7.pdf; Lynda C. Burton et al., *Using Electronic Health Records to Help Coordinate Care*, 82 MILBANK Q. 457, 461 (2004).

44. Burton et al., *supra* note 43, at 461.

decision support, or interoperability, all of which provide significant benefits to patients and clinicians.[45]

PHRs contain medical and claims information that is collected and maintained by patients who may then share this information with other parties, including employers, insurers, and private enterprises.[46] One source describes the PHR as follows:

> [A]n Internet-based set of tools that allows people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it. PHRs offer an integrated and comprehensive view of health information, including information people generate themselves such as symptoms and medication use, information from doctors such as diagnoses and test results, and information from their pharmacies and insurance companies. Individuals access their PHRs via the Internet, using state-of-the-art security and privacy controls . . . .[47]

Wal-Mart and other large employers, such as Intel and BP, with a total of 2.5 million employees, have formed a PHR system named Dossia.[48] Both Google and Microsoft have developed products that enable customers to maintain PHRs.[49]

However, stand-alone PHRs may be of limited use. To the extent data is entered by patients themselves, they may often be incomplete

---

45. *See supra* note 36 and accompanying text (discussing interoperability); *infra* Parts II.B.2, IV.C.2, and IV.C.5 (discussing computerized order entry, interoperability, and decision support).

46. Terry & Francis, *supra* note 11, at 688; *see also Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs*, 110th Cong. 5–6 (2007) [hereinafter *Private Health Records*] (testimony of Mark A. Rothstein, Director, University of Louisville School of Medicine), *available at* http://hsgac.senate.gov/public/_files/testimonyrothstien.pdf; Press Release, BlueCross BlueShield Association, BlueCross Introduces Personal Health Record for Fully-Insured Members (Sept. 20, 2006), *available at* http://www.bcbs.com/news/plans/bluecross-introduces-personal-health-records.html.

47. PERSONAL HEALTH WORKING GROUP, MARKLE FOUND., THE PERSONAL HEALTH WORKING GROUP FINAL REPORT 3 (2003), *available at* http://www.markle.org/downloadable_assets/final_phwg_report1.pdf.

48. *Private Health Records*, *supra* note 46, at 6.

49. *See* Steve Lohr, *Dr. Google and Dr. Microsoft*, N.Y. TIMES, Aug. 14, 2007, at C1; *see also* Martha Kessler, *Aetna Joins With Microsoft to Provide Portable Health Records for Members*, 16 BNA'S HEALTH CARE POL'Y REP. 1456 (2008); Google Health, http://www.google.com/health (last visted Dec. 19, 2008); Posting of Steve Lohr to NYTimes.com Bits Blog, Google Health Begins Its Preseason at Cleveland Clinic, http://bits.blogs.nytimes.com/2008/02/21/google-health-begins-its-preseason-at-cleveland-clinic (Feb. 21, 2008, 01:13 EST) (discussing a pilot project in which the health information of ten thousand Cleveland Clinic patients would be linked with Google PHRs).

or inaccurate.[50] Furthermore, without interoperability and the capacity to exchange data with EHR systems operated by all facilities at which the patient receives care, PHRs would constitute isolated and partial records, because they could not be accessed by all physicians and could not be updated with each new patient encounter.[51] Finally, stand-alone PHRs will not offer some of the most important benefits of EHR systems, including decision support and order entry. Consequently, some commentators assert that PHRs will be of significant benefit to patients and caregivers only if they are integrated into providers' EHR systems.[52]

B. Benefits of EHR Systems

Many experts have justifiably expressed strong enthusiasm for EHR systems, and many policy makers have asserted a commitment to promote their broad adoption.[53] These systems could facilitate clinicians' access to critical patient information and could prevent medical errors, thereby potentially saving thousands of lives and billions of dollars.[54]

This Section describes the numerous benefits of EHR systems, which could dramatically improve health care in the U.S. and worldwide. These benefits support the widespread adoption of EHR systems and the establishment of an NHIN.

1. Facilitating Access to Patients' Medical Records

EHR systems enable health care providers to obtain critical medical information about their patients as soon as the need for it arises. Essential to this capacity is interoperability.[55]

Interoperable EHR systems could allow doctors with proper authorization to access to relevant information about their patients, including medical histories, drug lists, and allergies, no matter where the patients had been previously treated. This capability could be invaluable in treating patients who arrive at the emergency room uncon-

---

50. Paul C. Tang et al., *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, 13 J. AM. MED. INFORMATICS ASS'N 121, 122 (2006) (asserting that "it is unlikely that individuals would keep records . . . up to date" and that "most patients cannot reliably report specific laboratory values such as their specific cholesterol level or hemoglobin A1c").

51. *Id.* at 124 (explaining that PHRs could "become 'information islands' that contain subsets of patients' data, isolated from other information about patients, with limited access and transient value").

52. *See, e.g.*, *id.* ("[A]ll the advantages of PHRs for providers depend on the PHR being integrated with the provider's EHR.").

53. *See supra* notes 10–14 and accompanying text.

54. *See* TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM, *supra* note 7, at 1–2.

55. *See supra* note 36 and accompanying text.

scious. It could also significantly facilitate and enhance the treatment of economically disadvantaged patients, who may not have attentive primary care physicians to manage their care[56] and who may not fully recall or understand the details of their medical histories.

Many patients who are not economically disadvantaged also have records that are fragmented and not fully accessible to all physicians treating them. According to one source, the average patient on Medicare visits seven different physicians every year.[57] If these doctors do not communicate and carefully coordinate the patient's care, any one of them may miss vital information that is critical to the individual's welfare.

An additional strength of EHRs is that, if appropriately backed up or replicated, they should be less vulnerable to loss or destruction than paper records. This problem with paper records was highlighted in the aftermath of Hurricane Katrina, when the medical records of many displaced New Orleans residents were destroyed.[58]

2. Improving Quality of Care and Reducing Poor Treatment Decisions

EHR systems can reduce errors and thereby improve patient safety, particularly through decision support features.[59] Decision support is "any information added by a system to assist the clinician's decision-making process."[60] EHR systems can incorporate reminders, prompts, and links to medical literature to promote accurate, timely, and responsible care.[61] Studies have shown that computerized re-

56. *See* Lawrence O. Gostin, *"Police" Powers and Public Health Paternalism: HIV and Diabetes Surveillance*, 37 HASTINGS CENTER REP. 9, 10 (2007) ("Most poor people do not enjoy the benefits of education and income that enable them to form stable physician-patient relationships and comply with complex treatment regimes.").

57. DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., IMPROVING HEALTH CARE: WHY A DOSE OF IT MAY BE JUST WHAT THE DOCTOR ORDERED 3 (2007), *available at* http://www.itif.org/files/HealthIT.pdf.

58. *See* Olga Pierce, *Analysis: The Medical Record Paper Chase*, UPI, Sept. 15, 2006, LEXIS, News Library, UPI File; *see also* Jeff Day, *Group Finds Support for E-Health Records, 'Medical Home' Clinics Following Hurricane*, 15 BNA'S HEALTH CARE POL'Y REP. 716, 716 (2007).

59. *See* Basit Chaudhry et al., *Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care*, 144 ANNALS INTERNAL MED. 742, 748 (2006) (citing the benefits of "increased delivery of care based on guidelines . . . , reduction of medication errors, and decreased rates of utilization for potentially redundant or inappropriate care"); *see also* INST. OF MED., *supra* note 2, at 5. But see *infra* Part II.C.1 for discussion of the possibility that EHR systems might sometimes cause errors instead of preventing them.

60. Jonathan A. Handler et al., *Computerized Physician Order Entry and Online Decision Support*, 11 ACAD. EMERGENCY MED. 1135, 1135 (2004).

61. *See* Anne Bobb et al., *The Epidemiology of Prescribing Errors: The Potential Impact of Computerized Prescriber Order Entry*, 164 ARCHIVES INTERNAL MED. 785, 788–89 (2004); Richard Hillestad et al., *Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs*, 24 HEALTH AFF. 1103, 1110 (2005);

minder systems improve immunization rates, preventive care, clinician adherence to practice guidelines, and the thoroughness of patient histories. Studies have also shown that EHR systems reduce prescribing costs, prescribing mistakes, and unneeded diagnostic tests.[62] According to one source, computerized physician order entry ("CPOE") systems could likely prevent sixty-five percent of prescribing errors, largely by incorporating decision support features that would educate doctors about medications.[63] In one instance, for example, a doctor typed a prescription for ten times the proper dosage, and the EHR system informed him of the error.[64]

EHR systems might also dissuade physicians from practicing wasteful "defensive medicine."[65] Clinicians could rely on decision support mechanisms to determine whether particular diagnostic procedures or treatments are warranted. Because these mechanisms would be designed based on widely accepted medical practices, the doctors could, if necessary, cite their reliance on the mechanisms to defend their medical decisions.

Likewise, the systems could reduce the unnecessary use of antibiotics. One study found that seventy-three percent of adults who visit primary care physicians for sore throats are treated with antibiotics, even though only five to seventeen percent of adults' sore throats re-

---

Jeffrey A. Linder, *Health Information Technology as a Tool to Improve Care for Acute Respiratory Infections*, 10 AM. J. MANAGED CARE 661, 661 (2004).

62. *See* Burton et al., *supra* note 43, at 461, 464; *see also* Paul R. Dexter et al., *A Computerized Reminder System to Increase the Use of Preventive Care for Hospitalized Patients*, 345 NEW ENG. J. MED. 965, 968 (2001) (finding that "the use of reminders increased the use of pneumococcal and influenza vaccination from practically zero to approximately 35 percent and 50 percent, respectively" for hospitalized patients); Elizabeth Mitchell & Frank Sullivan, *A Descriptive Feast but an Evaluative Famine: Systematic Review of Published Articles on Primary Care Computing During 1980–97*, 322 BRIT. MED. J. 279, 281 (2001) (describing "improvements in immunisations and preventive care and reductions in prescribing costs and unnecessary tests" due to computerization); Mike Pringle, *Using Computers to Take Patient Histories*, 297 BRIT. MED. J. 697, 697 (1988) ("Computer histories are more exhaustive than those taken in the normal way."); Charles Safran et al., *Guidelines for Management of HIV Infection with Computer-Based Patient's Records*, 346 LANCET 341, 344 (1995) (concluding that EHR systems help clinicians to adhere to practice guidelines).

63. Bobb et al., *supra* note 61, at 788.

64. Ceci Connolly, *Cedars-Sinai Doctors Cling to Pen and Paper*, WASH. POST, Mar. 21, 2005, at A01.

65. *See* David M. Studdert et al., *Defensive Medicine Among High-Risk Specialist Physicians in a Volatile Malpractice Environment*, 293 JAMA 2609, 2609 (2005) (noting that defensive medicine is prevalent among Philadelphia physicians in specialties with a high risk of litigation). "Defensive medicine" is the practice of making healthcare decisions "with the sole intention of preventing" malpractice lawsuits and can include the provision of excessive unnecessary care or the avoidance of beneficial treatment that is high-risk. G.D. Dalton et al., *Effect of Physician Strategies for Coping with the US Medical Malpractise Crisis on Healthcare Delivery and Patient Access to Healthcare*, 122 PUB. HEALTH 1051, 1054–55 (2008).

quire antibiotic therapy.[66] The excessive use of broad spectrum antibiotics has led to the emergence of antibiotic-resistant bacteria.[67] This phenomenon might become less common with the assistance of decision support systems designed to provide guidance concerning prescription drugs.

Currently, the lag between the discovery of new treatments and their consistent use in medical practice can be up to twenty years.[68] EHR systems, however, could significantly expedite the broad dissemination of knowledge about effective new treatments through decision support mechanisms.[69]

Furthermore, by allowing physicians to search patient records electronically for the information they require, EHR systems can reduce the amount of time providers spend reviewing patients' medical histories.[70] In addition, electronic searches can allow clinicians to identify patients who should be informed about matters such as drug recalls.[71]

Of particular significance is the potential role of these systems in reducing health disparities in the U.S.[72] Health disparities between whites and blacks have been the subject of much commentary and debate in recent years.[73] Technology that provides resource-poor practices with automatic decision support, reminders, and alerts based on the most advanced medical knowledge could enhance the care available to economically disadvantaged patients. With affordable or sub-

---

66. Jeffrey A. Linder & Randall S. Stafford, *Antibiotic Treatment of Adults With Sore Throat by Community Primary Care Physicians: A National Survey 1989–1999*, 286 JAMA 1181, 1185 (2001) (providing statistics regarding the use of antibiotics); *see also* Richard E. Besser, Editorial, *Antimicrobial Prescribing in the United States: Good News, Bad News*, 138 ANNALS INTERNAL MED. 605, 605 (2003) ("[I]n 1992, the U.S. Centers for Disease Control and Prevention (CDC) stated that over 40% of antimicrobial courses prescribed in physicians' offices were inappropriate.").

67. *See* Besser, *supra* note 66, at 605.

68. COMM. ON QUALITY OF HEALTH CARE IN AM., INST. OF MED., CROSSING THE QUALITY CHASM: A NEW HEALTH SYSTEM FOR THE 21ST CENTURY 145 (2001) [hereinafter CROSSING THE QUALITY CHASM].

69. *See* Louise Liang, *The Gap Between Evidence and Practice*, 26 HEALTH AFF. w119, w120 (2007).

70. *See* Richard J. Baron et al., *Electronic Health Records: Just Around the Corner? Or over the Cliff?*, 143 ANNALS INTERNAL MED. 222, 225–26 (2005).

71. *See id.*

72. *See* Alexandra E. Shields et al., *Adoption of Health Information Technology in Community Health Centers: Results of a National Survey*, 26 HEALTH AFF. 1373, 1381 (2007) (stating that expanding HIT capacity "seems a valuable strategy to further reduce health disparities for a substantial number of financially vulnerable patients").

73. *See, e.g.*, René Bowser, *Racial Profiling in Health Care: An Institutional Analysis of Medical Treatment Disparities*, 7 MICH. J. RACE & L. 79, 81 (2001) (positing an institutional basis for white-black disparities in medical treatment); Ichiro Kawachi et al., *Health Disparities by Race and Class: Why Both Matter*, 24 HEALTH AFF. 343 (2005) (examining racial and class disparities in health); David Satcher et al., *What if We Were Equal? A Comparison of the Black-White Mortality Gap in 1960 and 2000*, 24 HEALTH AFF. 459 (2005) (discussing persistent racial inequalities in standardized mortality ratios over a forty year period).

sidized EHR systems, clinicians who are pressed for time and resources would have information at their fingertips that they might otherwise be unable to access. It must be noted, however, that, if only wealthy practices can afford EHR systems and others are left without the improvements they enable, the technology could increase health disparities between rich and poor communities. Consequently, it will be important to offer financial support for EHR system adoption to some practices.[74]

EHR systems also have much to contribute to public health emergency response efforts. EHR vendors[75] and public health officials could use decision support functions in EHR systems to inform clinicians as to how best to respond to public health emergencies.[76] For example, EHR systems nationwide might be quickly reconfigured to advise caregivers to treat patients with particular symptoms as possible carriers of an emerging infectious disease.

3. Cost Savings

Many commentators associate significant cost savings with EHR systems, despite the expenses of purchasing, implementing, and operating them.[77] Some commentators have estimated the net economic benefits of EHR implementation to range from $8400 to $140,100 per physician over five years.[78] Others have found savings of $16.7 million over ten years for a hospital operating a CPOE system.[79] Still others have estimated $77.8 billion a year in savings for the institution of a standardized, interoperable national system.[80] These cost savings result from the following: fewer duplicated tests; reduction in administrative expenditures; a decrease in medical errors and adverse drug events linked to ignorance about the patient's allergies, medical history, and other prescription drugs; and, from the provider's perspec-

74. *See infra* Part IV.A.1.

75. Throughout this Article we use the term "vendor" broadly to refer to those who develop or modify EHR system software, install it, or integrate it with existing systems. Health care providers who perform these functions themselves should be deemed vendors for legal purposes relating to EHR system activities ordinarily performed by vendors.

76. These adaptations could be similar to automatic anti-virus downloads, which are now commonly available.

77. See *infra* notes 131–33 and accompanying text for discussion of these costs.

78. William W. Stead, *Rethinking Electronic Health Records to Better Achieve Quality and Safety Goals*, 58 ANN. REV. MED. 35, 37 (2007).

79. Rainu Kaushal et al., *Return on Investment for a Computerized Physician Order Entry System*, 13 J. AM. MED. INFORMATICS ASS'N 261, 265 (2006).

80. Jan Walker et al., *The Value of Health Care Information Exchange and Interoperability*, 25 HEALTH AFF. W5-10, W5-16 (2005). For a critique of estimates of savings generated by the proposed NHIN, see CONG. BUDGET OFFICE, EVIDENCE ON THE COSTS AND BENEFITS OF HEALTH INFORMATION TECHNOLOGY 8 (2008), *available at* http://www.cbo.gov/ftpdocs/91xx/doc9168/05-20-HealthIT.pdf (discussing "estimates of the potential net benefits that could arise nationwide if all providers and hospitals adopted health information technology").

tive, from improved mechanisms for calculating and recording charges.[81] Doctors would be able to retrieve the EHRs of patients who present at emergency rooms no matter where those records are housed and thus would not need to conduct diagnostic tests that the patient has already recently undergone. Furthermore, access to a patient's complete EHR, including medical history, allergies, and current medication list, could prevent medical errors in the emergency room that might lead to lengthy hospitalization, surgery, and other expensive care.

Other commentators note, however, that to date there is a dearth of compelling empirical evidence that proves the cost-effectiveness of EHR systems.[82] Indeed, because of the relatively low rate of EHR system adoption, to date there is only limited data concerning cost savings.[83] The evidence base is likely to improve as more institutions adopt EHR systems and an increasing number of researchers and economists begin to study their impact.

4. Promoting Research

EHRs could also promote medical research and the collection of much needed evidence concerning the efficacy of various treatment alternatives.[84] The term of art for decision-making rooted in scientific knowledge is "evidence-based medicine,"[85] a concept that is now frequently discussed in academic and scientific circles.[86] First, EHRs could facilitate the identification of patients for clinical studies by allowing investigators to search their patient records electronically for individuals who meet the inclusion criteria for particular clinical trials. Second, many studies could be based directly on analysis of the

81. *See* CONG. BUDGET OFFICE, *supra* note 80; Kaushal et al., *supra* note 79, at 263 tbl.1; Walker et al., *supra* note 80, at W5-16.

82. S. Clamp & J. Keen, *Electronic Health Records: Is the Evidence Base Any Use?*, 32 MED. INFORMATICS & INTERNET MED. 5, 9 (2007) (stating that the authors "found no technically sound evidence about cost changes associated with EHR").

83. Hillestad et al., *supra* note 61, at 1104 ("[T]he currently useful evidence [concerning HIT efficiency savings] is not robust enough to make strong predictions . . . .").

84. *See* sources cited *infra* notes 385–87 (discussing the uncertainty surrounding many medical decisions).

85. *See* Marc A. Rodwin, *The Politics of Evidence-Based Medicine*, 26 J. HEALTH POL. POL'Y & L. 439, 439 (2001) (explaining that "[e]vidence-based medicine is portrayed as an alternative to medicine based on authority, tradition, and the physician's personal experience" and that it involves evaluating the "safety, effectiveness, and cost of medical practices using tools from science and social science").

86. *See, e.g.*, Scott R. Sehon & Donald E. Stanley, *A Philosophical Analysis of the Evidence-Based Medicine Debate*, 3 BMC HEALTH SERVICES RES. (2003), http://www.biomedcentral.com/1472-6963/3/14 (arguing that the medical community must clarify the "nature of [evidence-based medicine] and its relationship to alternative approaches to medicine").

extensive and comprehensive data contained in electronic records.[87] EHR systems should facilitate efficient and extensive collection of evidence and development of new knowledge.[88]

Randomized, controlled clinical trials are considered the gold standard of medical studies.[89] However, research can also be accomplished through observational studies, which could be facilitated by the use of EHRs.[90] Rather than conducting a controlled experiment, investigators might review the charts or electronic files of patients receiving different medications or different types of surgery to treat a particular condition in order to determine the efficacy of each approach.[91]

At times, observational studies may be skewed by uncontrolled variables, such as changes in diet, exercise, stress level, or other lifestyle modifications that are not noted in the record and of which researchers remain unaware.[92] However, observational studies may also have several advantages over clinical trials. Interoperable systems can allow researchers to access vast amounts of information about various subpopulations over long periods of time.[93] Researchers can monitor patients for years after drugs have been approved by the FDA and detect patterns of adverse events, avoiding continued harm to patients

87. *See* John Powell & Iain Buchan, *Electronic Health Records Should Support Clinical Research*, 7 J. MED. INTERNET RES. (2005), *available at* http://www.jmir.org/2005/1/e4/.

88. Liang, *supra* note 69, at w120.

89. Friedrich K. Port, *Role of Observational Studies Versus Clinical Trials in ESRD Research*, 57 KIDNEY INT'L (SUPPLEMENT 74) S3, S3 (2000), *available at* http://www.nature.com/ki/journal/v57/n74s/pdf/4491615a.pdf ("Randomized controlled clinical trials have been considered by many to be the only reliable source for information in health services research."). Experimental studies involve "the collection of data on a process when there is some manipulation of variables that are assumed to affect the outcome of a process, keeping other variables constant as far as possible." BRYAN F.J. MANLY, THE DESIGN AND ANALYSIS OF RESEARCH STUDIES 1 (1992).

90. CHARLES P. FRIEDMAN & JEREMY C. WYATT, EVALUATION METHODS IN BIOMEDICAL INFORMATICS 369 (2d ed. 2006) (defining an observational study as an "[a]pproach to study design that entails no experimental manipulation" in which "[i]nvestigators typically draw conclusions by carefully observing [subjects] with or without an information resource"); MANLY, *supra* note 89, at 1 (explaining that observational studies involve the collection of data "by observing some process which may not be well-understood").

91. *See, e.g.*, Kjell Benson & Arthur J. Hartz, *A Comparison of Observational Studies and Randomized, Controlled Trials*, 342 NEW ENG. J. MED. 1878, 1879–83 (2000).

92. *See* MANLY, *supra* note 89, at 4–5 ("[A] prima facie conclusion may be invalid because of the *confounding* effects of uncontrolled variables."); Benson & Hartz, *supra* note 91, at 1878 ("Concern about inherent bias [in observational studies] has limited their use in comparing treatments."); Gary Taubes, *Do We Really Know What Makes Us Healthy?*, N.Y. TIMES, Sept. 16, 2007, § 6 (Magazine), at 52 (describing the limitations of observational studies and stating that they "can only provide what researchers call hypothesis-generating evidence — what a defense attorney would call circumstantial evidence").

93. *See* Liang, *supra* note 69, at w120 ("EHRs have the potential to take over where clinical trials and evidence-based research leave off, by providing real-world evidence of drugs' and treatments' effectiveness across subpopulations and over longer periods of time.").

such as that caused by ignorance about the side effects of Vioxx.[94] These studies can also be considerably less costly and time-consuming than experimental research because the data used already exists[95] and investigators need not comply with federal research regulations nor obtain approval from Institutional Review Boards ("IRBs")[96] if records are de-identified.[97] In addition, investigators could study the cases of individuals with very rare diseases that cannot be studied through large-scale clinical trials. Likewise, researchers could review the records of patients who receive care of varying quality, including substandard care. Such substandard care, which is at times provided in real world treatment settings, would not be provided in the controlled setting of a clinical trial.

It is not anticipated that EHR-based observational studies would replace randomized clinical trials.[98] However, observational studies are a valuable addition to the research toolkit.[99] In the words of one commentator, EHRs "will offer the capacity for real-time learning from the experience of tens of millions of people and will greatly increase the ability to generate and test hypotheses."[100]

C. The Challenges of EHR System Implementation

Despite the many potential benefits of EHR systems, they are not an unalloyed good. Their design, implementation, use, and maintenance raise important concerns that must not be overlooked. EHR system failures can cause significant injury and cost lives. Unauthorized disclosure of electronic health information can also lead to large scale privacy breaches, and the cost of implementing EHR systems may threaten the financial viability of some medical practices. The risks generated by these complex software systems are sufficiently serious that they demand regulatory oversight.[101]

---

94. Lynn M. Etheredge, *A Rapid-Learning Health System*, 26 HEALTH AFF. w107, w111 (2007).

95. Benson & Hartz, *supra* note 91, at 1878; Port, *supra* note 89, at S3.

96. 21 C.F.R. § 56.102(g) (2007) ("*Institutional Review Board (IRB)* means any board, committee, or other group formally designated by an institution to review, to approve the initiation of, and to conduct periodic review of, biomedical research involving human subjects.").

97. *See infra* note 393 and accompanying text (discussing regulatory requirements for the approval of research studies).

98. *See, e.g.*, Etheredge, *supra* note 94, at w108.

99. *See* Port, *supra* note 89, at S5 (arguing that both observational studies and clinical studies have their place and complement each other); *see also* Jerry Avorn, *In Defense of Pharmacoepidemiology — Embracing the Yin and Yang of Drug Research*, 357 NEW ENG. J. MED. 2219, 2220 (2007) (listing the strengths and weaknesses of clinical and observational studies of medications); Benson & Hartz, *supra* note 91, at 1878, 1884 (concluding, based on a literature review, that "observational studies and randomized controlled trials usually produce similar results").

100. Etheredge, *supra* note 94, at w108.

101. *See infra* Part III.A.2 (arguing for regulatory oversight of EHR systems).

1. Potential for Errors

In some instances, EHR systems may generate errors rather than prevent them, especially early in the adoption process.[102] Many of these errors could significantly harm patients. One study of a hospital's CPOE system identified twenty-two circumstances in which CPOE increased rather than decreased the likelihood of error.[103] Sources of such errors include: fragmentation of data; failure to integrate all hospital systems; and human-computer interface difficulties rooted in the machine rules' failure to reflect work organization or expected provider behavior.[104] For example, errors can result from computer crashes or from maintenance shutdowns that lead to lost orders.[105] They may also result from system inflexibilities that significantly impede providers' ability to enter nonstandard specifications or to order non-formulary medications.[106] Usability problems, such as display and navigation deficiencies, can also cause errors.[107]

Furthermore, complex software systems invariably exhibit a significant degree of coupling or interdependence between their many components. Consequently, a failure of one component may cause or contribute to the failure of another component that is not obviously related to the first component.[108] Similarly, complex software sometimes fails unpredictably due to unforeseen or untested interactions between its various features and services.[109] Under certain conditions, a clearly safety-critical component of an EHR system, such as a diagnostic aid for cardiac care, might function incorrectly because of a

102. *See* Stead, *supra* note 78, at 38.

103. Ross Koppel et al., *Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors*, 293 JAMA 1197, 1199–201 (2005).

104. Stead, *supra* note 78, at 38 (discussing human-computer interface problems); *see* Jonathan R. Nebeker et al., *High Rates of Adverse Drug Events in a Highly Computerized Hospital*, 165 ARCHIVES INTERNAL MED. 1111, 1114–15 (2005) (finding high rates of error at a hospital whose CPOE system did not have adequate decision support); Robert L. Wears, *Computer Technology and Clinical Work*, 293 JAMA 1261, 1262 (2005) (explaining that "the model of health care work inscribed" in CPOE and decision support systems clashes "with the actual nature of clinical work").

105. Koppel et. al., *supra* note 103, at 1201.

106. *Id.* Nonformulary medications are "[d]rugs not on a [health care] plan-approved drug list." Medicare.gov — Glossary Definitions, http://www.medicare.gov/Glossary/search.asp?SelectAlphabet=N&Language=English#Content (last visited Dec. 19, 2008).

107. *See* Hartzband & Groopman, *supra* note 16, at 1657.

108. *See* John Rushby, *Critical System Properties: Survey and Taxonomy*, 43 RELIABILITY ENGINEERING & SYS. SAFETY 189, 210 (1994) (discussing coupling and explaining how tightness of coupling promotes efficiency but can cause unexpected failures in various system components).

109. Dirk O. Keck & Paul J. Kuehn, *The Feature and Service Interaction Problem in Telecommunications Systems: A Survey*, 24 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 779, 779–80 (1998).

subtle interaction with an apparently unrelated defective component, such as a billing feature.[110]

Other errors may cause physicians to absorb financial losses. One physician reported that billing interface errors caused many of his patients to be improperly categorized as established rather than new patients, which resulted in a $90,000 revenue loss.[111]

Some failures caused by flawed software design, implementation, or validation could be avoided with improved software engineering practices.[112] However, as EHR system functionality becomes more complex, the safety risks to patients may grow unless additional quality control interventions are initiated.[113]

2. Privacy and Security Concerns

Both patients and analysts have expressed concern that EHR systems will threaten patient privacy and be vulnerable to security breaches.[114] With a fully interoperable NHIN, EHRs could be accessed from anywhere in the country and transmitted illicitly across the world quickly, cheaply, and with little risk of detection.[115] The security of health information is, in fact, compromised with alarming frequency as a result of computer theft, sale of used computers without removal of data from hard drives, hacking, inadvertent disclosures, and deliberate misuse of information by those with access to it.[116] As an example, Georgetown University Hospital suspended a test program with electronic prescription provider InstantDx after a serious security breach was discovered in 2006.[117] The hospital had

---

110. Undesirable coupling and complex interactions between software components can be reduced by the application of certain software design techniques such as object-oriented design, but dependencies between components are an inherent aspect of software systems and cannot be eliminated or rendered insignificant. ERICH GAMMA ET AL., DESIGN PATTERNS: ELEMENTS OF REUSABLE OBJECT-ORIENTED SOFTWARE 24–25 (1999) (discussing design patterns that reduce coupling).

111. Ken Terry, *IT Implementation: Why EHRs Falter*, MED. ECON., April 7, 2006, at 44, *available at* http://www.memag.com/memag/content/printContentPopup.jsp?id=316528.

112. Madhavan Nayar & Sharon Miller, *Anticipating Error: Identifying Weak Links in the Electronic Healthcare Environment*, 75 J. AM. HEALTH INFO. MGMT. ASS'N 46, 47–49 (2004) (discussing various factors that are intrinsic and extrinsic to EHR systems and create risks of error).

113. *See infra* Parts IV.B and IV.C for recommendations.

114. Terry & Francis, *supra* note 11, at 696; National Committee on Vital and Health Statistics, Privacy and Confidentiality in the Nationwide Health Information Network 8–13 (June 22, 2006), http://ncvhs.hhs.gov/060622lt.htm [hereinafter NCVHS] ("Protecting the confidentiality of personal health information in such settings requires institutions to establish different access rules depending on employees' responsibilities and their need to know the information to carry out their role.").

115. Sharona Hoffman & Andy Podgurski, *Securing the HIPAA Security Rule*, J. INTERNET L., Feb. 2007, at 1, 6.

116. *Id.* at 6.

117. Kevin Poulsen, *E-Health Gaffe Exposes Hospital*, WIRED, July 25, 2006, http://www.wired.com/science/discoveries/news/2006/07/71453.

securely transmitted data concerning thousands of patients to InstantDx, but, because of InstantDx's flawed security practices, an Indiana consultant was able accidentally to stumble upon the online files while installing medical software for a client.[118]

To address privacy and security concerns related to personal health information, the U.S. Department of Health and Human Services ("HHS") promulgated the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule[119] and the HIPAA Security Rule,[120] the latter of which governs the security of certain electronic health information.[121] We have critiqued these regulations at length in prior work and noted their shortcomings.[122] The Privacy Rule covers only a narrow range of entities, namely health plans, health care clearinghouses, and health care providers who transmit health information electronically for claims, billing, or health plan purposes.[123] It does not cover employers, marketers, life insurers, or many others who might handle personal health information. The Privacy Rule also does not feature a private cause of action,[124] so its deterrent and remedial effects are limited.[125] In addition, the Security Rule's standards are extremely vague, leaving a vacuum of guidance that makes meaningful compliance unlikely.[126] A 2007 assessment of HIPAA compliance in fact found widespread confusion and mistakes.[127] The standards in the HIPAA Privacy and Security Rules must be clarified, and their enforcement must be bolstered so that patient privacy and EHR confidentiality are meaningfully protected.[128]

---

118. *Id.*

119. 45 C.F.R. §§ 160.101–.534 (2007).

120. *Id.* §§ 160.302–.318.

121. *See* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 338–44 (2007) (discussing the HIPAA Security Rule).

122. *Id.* at 344–59.

123. 45 C.F.R. § 160.103.

124. *Id.* §§ 160.300–.552.

125. As of December 31, 2007, HHS received 32,487 complaints of HIPAA Privacy Rule violations. *See* Privacy — Compliance and Enforcement, http://www.hhs.gov/ocr/privacy/enforcement/numbersglance.html (last visited Dec. 19, 2008). However, no civil fines had been imposed, and only four criminal actions had been brought under HIPAA's criminal enforcement provision. *See* Tresa Baldas, *Hospitals Fear Privacy Claims Over Medical Records*, NAT'L L.J., May 28, 2007, at 4, 4.

126. Hoffman & Podgurski, *supra* note 121, at 350–54.

127. *HIPAA Compliance Strategies: National Review of HIPAA Compliance Finds Rampant Confusion, Mistakes*, REP. ON PATIENT PRIVACY (Atl. Info. Servs., Inc., Washington, D.C.), May 2007, *available at* http://www.aishealth.com/Compliance/Hipaa/RPP_National_Review_Rampant_Mistakes.html.

128. Hoffman & Podgurski, *supra* note 121, at 359–84 (developing recommendations for the improvement of the HIPAA Privacy and Security Rules). A recently proposed bill, the Health-e Information Technology Act, H.R. 6898, 110th Cong. §§ 400–15 (2008), would bolster privacy and security safeguards. *See* THE HON. PETE STARK, CHAIRMAN, H. COMM. ON WAYS AND MEANS, SUBCOMM. ON HEALTH, PRIVACY AND SECURITY PROVISIONS OF

Many states also have medical confidentiality rules that will affect EHR systems.[129] Because the NHIN would be an interstate network allowing data that is entered in one location to be accessed anywhere in the U.S., some of the state standards may cause significant complications and require modification in light of HIT developments.[130]

3. Expense, Time, and Burden

The introduction of EHR systems into medical practice can involve significant costs and difficulties. The purchase of an EHR system is estimated to cost $33,000 per doctor, with an additional $1500 a month per doctor for maintenance.[131] According to a study of Pennsylvania hospitals, the median capital spending per bed for HIT in 2006 was $6912, while the median HIT operating cost per bed was $14,528.[132] The cost of achieving a fully interoperable NHIN has been estimated at $156 billion in capital investment and $48 billion in yearly operating expenses over five years.[133]

Transitioning to an EHR system can also place significant administrative burdens upon health care providers. The potential difficulties of EHR implementation include all of the following: (1) office systems must be redesigned; (2) users must adopt uniform ways of recording data to fit system requirements and must forego their own shorthand and terminology; (3) data from paper records must be en-

---

HEALTH-E IT ACT OF 2008 (Comm. Print 2008), *available at* http://www.house.gov/stark/news/110th/legislation/200809-HIT/privacy.pdf.

129. CARL H. COLEMAN ET AL., THE ETHICS AND REGULATION OF RESEARCH WITH HUMAN SUBJECTS 446–47 (2005) (discussing state medical confidentiality laws); *see, e.g.*, N.Y. PUB. HEALTH LAW § 17 (McKinney 2002) (prohibiting disclosure of a minor's medical records concerning abortion and sexually transmitted diseases without the minor's consent); 71 PA. CONS. STAT. ANN. § 1690.108 (West 1990) (prohibiting disclosure of records prepared during drug and alcohol abuse treatment); *see also* Health Privacy — State Law, http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat_search.htm (last visited Dec. 19, 2008) (summarizing and providing links to the health information privacy laws of each state).

130. Terry & Francis, *supra* note 11, at 709–10 (discussing how state laws can present challenges for a national EHR system); NCVHS, *supra* note 114, at 9 (describing the confusion, difficulty, and expense of designing a national health information network to comply with numerous health privacy laws enacted by the states).

131. Thomas Goetz, Editorial, *Physician, Upgrade Thyself*, N.Y. TIMES, May 30, 2007, at A21; *see also* Baron et al., *supra* note 70, at 223–24 (reporting that an EHR system cost a four-person medical practice $140,000, including hardware, software, training, and one year of support, and estimating the system's annual maintenance cost, including support services, to be $40,000).

132. HOSP. & HEALTHSYSTEM ASS'N PA., IMPROVING PATIENT CARE: PENNSYLVANIA HOSPITALS' USE OF INFORMATION TECHNOLOGY 4 (2007), *available at* http://www.haponline.org/downloads/Improving_Patient_Care_PA_Hospitals_Use_of_IT_HAP_082007.pdf. Capital costs include buildings, medical equipment, and EHR systems, while operating costs include the daily expenses of running a hospital. *Id.*

133. Rainu Kaushal et al., *The Costs of a National Health Information Network*, 143 ANNALS INTERNAL MED. 165, 170 (2005).

tered into the electronic system; (4) all staff members must learn to be proficient with the system, and their training takes time away from patient care; and (5) patients may be concerned about providers spending considerable time inputting data into computers during examinations, leaving less time for human interaction between the clinician and the individual being examined.[134]

Even in the long term, use of EHR systems may be time consuming for providers.[135] Typing may take physicians longer than dictating notes.[136] One study found that, during consultation, use of EHRs increased the time that doctors spent on activities other than interacting with patients by as much as twenty-eight percent and that this did not change with improved computer proficiency.[137] Other writers have noted that, in the intensive care unit, where numerous interventions must be performed in rapid succession, CPOE systems may increase mortality because staff members must spend significant time at computer terminals rather than at the bedside.[138] How time consuming and problematic an EHR system is, however, depends largely upon its user interface design.[139] Enhanced designs, including mechanisms such as voice recognition software, allow users to operate systems more quickly and more safely.[140]

4. Legal Issues

Use of EHR systems may raise important tort litigation questions.[141] Addressing all of the issues in detail is beyond the scope of this Article, but some bear mentioning. For example, to what extent

134. *See, e.g.*, Baron et al., *supra* note 70, at 223–24 (describing the difficulties one practice faced in implementing a new EHR system); Connolly, *supra* note 64 (relating that Cedars-Sinai Medical Center in Los Angeles abandoned its $34 million EHR system after staff members found that it was "clunky and slow" and that they could not operate it effectively, because they had received insufficient training); Terry, *supra* note 111 (describing difficulties associated with EHR implementation).

135. Yong Y. Han et al., *Unexpected Increased Mortality After Implementation of a Commercially Sold Computerized Physician Order Entry System*, 116 PEDIATRICS 1506, 1510 (2005) (asserting that CPOE systems require more time for order entry than written forms, although this may be mitigated by improved overall efficiency).

136. *See* Baron et al., *supra* note 70, at 223–24 (discussing increases in patient waiting times due to the adoption of an EHR system).

137. Mitchell & Sullivan, *supra* note 62, at 281.

138. *See, e.g.*, Han et al., *supra* note 135, at 1510.

139. *See* Michael E. Wiklund, *Making Medical Device Interfaces More User-Friendly*, *in* DESIGNING USABILITY INTO MEDICAL PRODUCTS 151–60 (Michael E. Wiklund & Stephen B. Wilcox eds., 2005) (discussing user-interface problems and techniques for enhancing the user-friendliness of medical device interfaces).

140. *See id.*; Ken Terry, *Voice Recognition Moves Up a Notch: When the Computer Can Type While You Talk, You Save Money and Time*, MED. ECON., Feb. 20, 2004, at TCP11, *available at* http://www.memag.com/memag/Technology:+The+Connected+Physician/Voice-recognition-moves-up-a-notch/ArticleStandard/Article/detail/108559.

141. *See, e.g.*, Burton et al., *supra* note 43, at 465–66 (discussing the uncertainties regarding legal liability of physicians relying on data from other providers).

will a physician's reliance on guidance provided through decision support mechanisms insulate her from liability? Will EHR system vendors be included as a matter of course in every lawsuit because the provider's system might possibly have contributed to the alleged injury?[142] If so, will concern about litigation impede NHIN implementation, or will vendors demand immunity?[143] Will frequent attempts to prove failures in complex EHR systems through the testimony of costly expert witnesses drive the costs of litigation and malpractice insurance dramatically higher?

Furthermore, a patient harmed by a malfunction or security vulnerability of an EHR system may face difficulties proving her claims. The patient may find it very hard to establish that the system was responsible for her injuries unless the inputs provided to the system, the actions taken by users, and the outputs and actions generated by the system are faithfully recorded in a form that can be understood by an expert. It can be extremely challenging to inspect a complex EHR system's program code for the defect that was responsible for a failure that harmed a patient. Such a defect might involve only one line of code among many thousands.

Discovery issues might be particularly copious. For example, will printouts of EHRs accurately reflect the providers' activities? Will fragmented screen displays, physician shortcuts, and system inflexibilities impede discovery and distort the medical record?[144] Will EHRs record all of the providers' activities accurately, comprehensively, and chronologically, or will files be disjointed, confusing, and incomplete? Will e-mail messages exchanged between patients and physicians be captured by the EHR system and become part of the medical record?[145]

On the other hand, EHRs could significantly facilitate discovery of the truth in litigation. If all medical interventions are faithfully recorded in EHRs, computerized records will be much more comprehensive than paper files built upon dictation of physicians' summary notes. EHR systems could also ease the burdens of discovery by al-

142. *See* Arnold J. Rosoff, *On Being a Physician in the Electronic Age: Peering into the Mists at Point-&-Click Medicine*, 46 ST. LOUIS U. L.J. 111, 124–28 (2002) (discussing liability of developers of clinical decision-support software and justifiable reliance by physicians).

143. *See* ROBERT WOOD JOHNSON FOUND. ET AL., *supra* note 22, at 45 (noting that "immunity from suit is extremely rare" and that it is possible that HIT will generate new sources of liability).

144. *See supra* notes 102–13 and accompanying text (discussing the potential for errors generated by EHR systems).

145. *See* ROBERT WOOD JOHNSON FOUND. ET AL., *supra* note 22, at 45 ("To the extent that electronic technology makes the meaning of a medical record ambiguous, the scope of discovery could extend beyond the limits now imposed in paper medical record cases.").

lowing for electronic searches of medical files.[146] Both plaintiffs and defendants could use EHRs to their advantage in litigation.[147]

III. THE ROLE OF THE LAW AND ADMINISTRATIVE REGULATION

A. Why Are Legal Interventions Necessary?

EHR systems are not currently regulated by any governmental entity despite being crucial to the effective management of patient care in practices that use them.[148] There are at least two important reasons for governmental involvement in the realm of EHR systems. First, EHR systems are unlikely to be widely adopted in the near future without governmental intervention. The government should require all health care providers to adopt EHR systems and offer financial support to offset the providers' costs. Second, individual patients' lives and public health will depend on the proper functioning of EHR systems; therefore, like other goods and services that impact public welfare, EHR systems must be regulated.

1. Financial Support for Universal EHR System Adoption

Although many believe that EHR systems can dramatically improve the quality of health care in the U.S.,[149] the majority of health care providers have failed to adopt EHR systems thus far. According to a recent national survey, as of early 2008, only 4% of U.S. physicians in ambulatory care settings had fully functional EHR systems, and 13% had basic systems.[150] A 2008 survey of 3027 hospitals found that only 2% of hospitals have comprehensive EHR systems, though 19% of hospitals have basic EHR systems, and 75% record patient demographics and lab and radiology results electronically.[151] A 2006

146. *See* FED. R. CIV. P. 26(b)(2) advisory committee's note to 2006 amendments ("Electronic storage systems often make it easier to locate and retrieve information.").

147. *See infra* Part IV.C.3 (discussing audit trails and capture/replay and their potential role in litigation).

148. *See* Jason Miller, *FDA to Propose Rule on E-Health Records*, GOV'T HEALTH IT, June 5, 2007, http://www.govhealthit.com/online/news/102901-1.html (quoting Tim Stitely, the FDA's chief information officer, as stating that the FDA does not have jurisdiction to regulate EHRs and that he is uncertain as to which agency will regulate them).

149. *See supra* Part II.B (discussing the benefits of EHR systems).

150. DesRoches et al., *supra* note 6, at 54.

151. Jeff Day, *Comprehensive EHR Systems Rare in U.S. Hospitals, Researchers Tell Leavitt*, 16 BNA'S HEALTH CARE POL'Y REP. 1581, 1581 (2008). Comprehensive EHR Systems were defined as systems with twenty-four digitized operations, and basic EHR systems were defined as those with at least seven electronic functions. *Id.* The survey was funded by HHS and was "conducted in collaboration with the American Hospital Association." *Id.* A fall 2006 survey by the American Hospital Association had previously concluded that 11% of hospitals had fully implemented EHRs, while 57% had partially

study of community health centers showed that 26% asserted that they had some EHR capacity, and those serving largely poor and uninsured patients were unlikely to have any EHR capabilities.[152]

Commentators have, in fact, noted a misalignment of incentives. While providers must invest heavily in the purchase and maintenance of EHR systems, it is insurers and self-insured employers who will reap many of the systems' economic benefits: less frequent duplication of diagnostic tests and fewer medical errors that lead to costly complications.[153]

One way to compel the adoption of EHR systems is to establish a legal mandate requiring their use by all health care providers. We recommend that federal law include such a requirement, which should be phased in over a period of years, with longer deadlines for smaller practices.[154] Health care providers should be required to purchase and maintain EHR systems and also to make good faith use of their various components, including decision support, CPOE, and other capabilities. Federal regulations, consequently, should provide specific instructions as to what constitutes acceptable use.

Nevertheless, we also recognize that the imposition of such a mandate would be unjust without financial support for those who must bear the expense of fulfilling it. The federal government has already recognized the problem and begun addressing it through several initiatives. On August 1, 2006, the Centers for Medicare & Medicaid Services ("CMS") and the Office of the Inspector General adopted final regulations that create exceptions and safe harbors to federal fraud and abuse laws in order to encourage the donation of EHR systems.[155] The regulations establish the conditions under which entities

---

implemented EHRs, and that physicians in only 10% of hospitals routinely used CPOE at least half of the time. AM. HOSP. ASS'N, *supra* note 6, at 3, 5. Survey responses were received from over 1500 community hospitals, which constitute approximately one-third of all community hospitals in the U.S. *Id.* at 1. The survey also found that 46% of community hospitals made moderate or high use of HIT, including medication order entry, test result review, and clinical alert mechanisms, and that 51% of hospitals used real-time drug interaction alerts. *Id.*

152. Shields et al., *supra* note 72, at 1376. The survey also found that "only 13 percent [of community health centers] have the minimum set of functionalities defined by the national HIT Adoption Initiative." *Id.*

153. *See* Blackford Middleton et al., *Accelerating U.S. EHR Adoption: How to Get There from Here. Recommendations Based on the 2004 ACMI Retreat*, 12 J. AM. MED. INFORMATICS ASS'N 13, 14 (2005) (discussing "misaligned incentives"); David F. Doolan & David W. Bates, *Computerized Physician Order Entry Systems in Hospitals: Mandates and Incentives*, 21 HEALTH AFF. 180, 183–84 (2002) (discussing lack of financial incentives for provider implementation of EHR systems).

154. *Cf.* HIPAA Privacy Regulations, 45 C.F.R. §§ 164.318 & 164.534 (2007) (providing different compliance deadlines for various types of covered entities).

155. 42 C.F.R. § 411.357(v)-(w) (2007); *Id.* § 1001.952(x)-(y); *see* Press Release, U.S. Dep't of Health & Human Servs., New Regulations to Facilitate Adoption of Health Information Technology (Aug. 1, 2006), *available at* http://www.hhs.gov/news/press/2006pres/20060801.html.

may donate interoperable EHR and electronic prescribing hardware, software, information technology, and training without violating the physician self-referral law[156] and the federal anti-kickback statute.[157] The Internal Revenue Service has also recently issued a memo in which it established that nonprofit hospitals can provide EHR systems and support services to staff physicians without compromising their tax-exempt status.[158]

In addition, several congressional bills have been designed to offer various incentives to health care providers for the adoption of EHR systems. The proposed Wired for Health Care Quality Act of 2007 would provide $139 million in fiscal years 2008 and 2009, as well as further funding in subsequent years for HIT-related grants and loans to health care providers and to states.[159] Likewise, the Health-e Information Technology Act of 2008 proposes incentive payments of up to $40,000 over five years to physicians and several million dollars to hospitals for HIT adoption.[160] While such incentive programs may effectively encourage EHR system use, none of the proposed bills has passed thus far.[161]

2. The Need for Quality Control

The federal government must regulate EHR systems because their dependability and usability are crucial to patient welfare. A defect in the software of an EHR system containing hundreds or thousands of medical records, such as a flaw that causes inaccurate recording of patients' allergies or medications, could adversely affect a very large number of patients. The risk is amplified by the fact that EHR system functionality extends well beyond simple record keeping. Through features such as decision support and order entry, EHR systems already significantly influence the course of patients' treatments. More-

156. *See* 42 U.S.C. § 1395nn (2000 & Supp. V 2005), *amended by* Medicare Improvements for Patients and Providers Act of 2008, Pub. L. No. 110-275, 122 Stat. 2494.

157. *See* 41 U.S.C. §§ 51–58 (2006).

158. Memorandum from Lois G. Lerner, Exempt Organizations Director, Internal Revenue Service, Hospitals Providing Financial Assistance to Staff Physicians Involving Electronic Health Records (May 11, 2007), *available at* http://www.irs.gov/pub/irs-tege/ehrdirective.pdf.

159. Wired for Health Care Quality Act, S. 1693, 110th Cong. §§ 3008(a)(1), (b)(1), (e)(1) (2007); *see Senate HELP Committee Approves Health IT Legislation by Voice Vote*, 15 BNA'S HEALTH CARE POL'Y REP. 873 (2007) (reporting that the Senate Health, Education, Labor, and Pensions Committee approved the proposed legislation on June 27, 2007).

160. Health-e Information Technology Act, H.R. 6898, 110th Cong. §§ 301–302 (2008).

161. *Business Leaders, Senators Urge Action on Health IT Bill, Despite Privacy Concerns*, 16 BNA'S HEALTH CARE POL'Y REP. 457 (2008); Jeff Day, *Legislation to Advance EMR Adoption Unlikely to Move Before Mid-2009, Aide Says*, 16 BNA'S HEALTH CARE POL'Y REP. 1475 (2008) (explaining that "Congress is unlikely to take action on federal legislation that would pay doctors to adopt electronic medical record systems until well into 2009" because it will need to focus instead "on the economic crisis, the wars in Afghanistan and Iraq, and on passing fiscal year 2009 appropriations bills.").

over, it is possible that, before long, the analytical power of these systems will increase so much that they will assume a key role in medical diagnosis and treatment management.

The potentially devastating effect of system malfunctions is illustrated by the following incident. A hospital pharmacy's computer program generated erroneous medication order lists, leading to the delivery of the wrong drugs to patients in the wards.[162] Had the hospital staff not been vigilant and detected the mistakes, the consequences could have been catastrophic for some patients.[163]

A website entitled *Bad Health Informatics Can Kill* provides various examples of instances in which CPOE led to serious errors as well as other illustrations of how medical mistakes have been caused by technology, though not necessarily through EHR systems.[164] In truth, there is no way to know how many malfunctions have actually occurred because EHR systems are not subject to a governmentally mandated adverse-event-reporting requirement, unlike FDA-regulated drugs and devices.[165]

As noted earlier, the federal government has in fact begun to regulate electronic health information in the areas of privacy and security. HHS has enacted the HIPAA Privacy and Security Rules, under which a variety of requirements have been established for the use, disclosure, and protection of health information.[166] If the government is to protect patients' privacy through regulation of HIT, then surely it should also safeguard patients' health and safety by regulating the quality of EHR systems.

The federal government routinely regulates goods and services that impact public health and welfare. For example, the Department of Transportation regulates pipeline and hazardous material transport, railroads, motor carriers, cargo containers, highway traffic, and other transportation matters.[167] The Federal Aviation Administration ("FAA") regulates air traffic, air carriers, aircraft manufacturers, crewmembers, pilot schools, airports, and navigational facilities.[168]

Most relevant is the FDA's extensive regulation of drugs, devices, and biologics.[169] The term "device" is statutorily defined in relevant

---

162. Cook & O'Connor, *supra* note 17, at 80–82 (explaining that the problem was rooted in a backup tape that was incomplete and corrupted).

163. *Id.*

164. EFMI-WG Assessment of Health Information Systems, Bad Health Informatics Can Kill, http://iig.umit.at/efmi/badinformatics.htm (last visited Dec. 19, 2008).

165. *See* 21 C.F.R. § 803 (2007) (discussing FDA adverse event reporting requirements).

166. HIPAA Privacy Rule, 45 C.F.R. §§ 160.101–164.534 (2007); HIPAA Security Rule, *Id.* §§ 164.302–.318; *see* Hoffman & Podgurski, *supra* note 115; Hoffman & Podgurski, *supra* note 121; *supra* notes 115 and 121 and accompanying text (critiquing the Privacy and Security Rules).

167. *See* 49 C.F.R. §§ 1–1572.405 (2007) (transportation regulations).

168. *See* 14 C.F.R. §§ 1–198.17 (2007) (FAA regulations).

169. *See* 21 C.F.R. § 7.3(f) (2007) (defining "product" as "an article subject to the jurisdiction of the Food and Drug Administration, including any food, drug, and device intended

part as: "an instrument, apparatus, implement, machine . . . which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease."[170] Given that they feature decision support, order entry, and other care delivery and management functions, one might reasonably conclude that EHR systems are as essential to patient care as are many regulated devices.[171] Furthermore, their software can be more complicated than that found in many computer-controlled medical devices that are subject to FDA jurisdiction.[172]

Free market advocates might argue that EHR systems should remain unregulated because competitive market forces can safeguard their quality, as low-quality products will fail in the marketplace. This argument, however, is not persuasive for several reasons.[173]

First, government regulation is necessary to prevent market failure due to lack of information available to potential consumers. The market cannot weed out low-quality products if consumers are not informed about the relative quality of the various products available. Without a governmentally mandated adverse event reporting requirement, the public may never find out which products are defective or inferior to others, and thus they will be unable to make educated purchasing decisions. Vendors have little incentive to disclose product flaws to the public voluntarily. Complaints posted on Internet sites or blogs can be unreliable or technically imprecise and, therefore, may not be a trustworthy source for consumer advocacy groups interested in developing consumer reports. Health care providers who use EHR systems may hesitate to disclose adverse events suffered by patients that are associated with EHR systems because of the HIPAA Privacy Rule[174] or because of fear of lawsuits by vendors. In addition, even if users were inclined to report system defects to publicly available sources, they might still be slow to recognize emergent software problems because of their subtlety or complexity, and they may fail to un-

---

for human or animal use [or] any cosmetics and biologic intended for human use"). *See generally Id.* §§ 1–1405.670 (food and drug regulations).

170. 21 U.S.C. § 321(h) (2006).

171. *See* INST. OF MED., *supra* note 2, at 5 (noting that it is important to recognize the many uses of EHR systems, including care delivery, management, and support processes).

172. *See* Nayar & Miller, *supra* note 112, at 49 (discussing the complexity of EHR systems).

173. *Cf.* CHARLES P. FRIEDMAN & JEREMY C. WYATT, EVALUATION METHODS IN BIOMEDICAL INFORMATICS 357 (2d ed. 2006) ("[W]hile having been an entirely unregulated market in the past, the efficacy and safety of clinical information systems are increasingly attracting attention, creating new challenges, opportunities, and requirements for evaluation.").

174. 45 C.F.R. §§ 160.101–164.534 (2007). Clinicians would need to make sure that whatever information they convey about incidents does not identify particular patients and cannot be traced to specific individuals. *See id.* §§ 164.502–.514 (2007) (establishing regulations for the use and disclosure of protected health information).

derstand their significance.[175] Consequently, absent a carefully regulated approval process conducted by experts, many providers might purchase a new EHR system before its defects were widely known.

Second, market forces may be further thwarted by the fact that providers who have already invested in and implemented a faulty EHR system cannot readily take their business elsewhere. Once a provider has adopted an EHR system, it will be disinclined to switch to a new system, even if its current system is faulty. Such a switch could be prohibitively expensive and burdensome, as it would require transferring all existing patient records to a different product and training all staff members to adjust to the new product's peculiarities.

Third, while the threat of litigation might normally discourage sloppy software engineering, in the realm of complex HIT, liability might be so difficult to prove that vendors will believe they bear little risk of costly judgments or even of plaintiffs initiating suit.[176] Plaintiffs' attorneys will realize that they cannot prevail without well qualified experts who invest considerable time in studying the EHR system at issue. Therefore, lawyers may refuse to represent all but the wealthiest clients who can finance the retention of such experts without any certainty of recovering the costs through settlement or favorable judgments.

Finally, market forces alone cannot be trusted to ensure the interoperability of EHR systems, which is essential to the systems' efficacy. Interoperability would likely be disfavored by vendors because it could reduce profits and increase costs.[177] Although the earliest electronic hospital information systems emerged in the late 1960s,[178] interoperability has yet to be achieved, and no product has come close to gaining a monopoly that would eliminate the need for interoperability among competing products.[179] Furthermore, both the practice of customizing products to accommodate providers' preferences and the inherent complexity of representing medical information constitute potential obstacles to interoperability.[180] This important capacity will likely be achieved only through regulatory mandates.

---

175. *See infra* notes 193–94 and accompanying text (discussing the lengthy delays that can precede the emergence of a problem in a complex software system).

176. *See supra* Part II.C.4 (discussing proof and discovery problems); *infra* Part IV.C.3 (discussing recommendations that audit trails and capture/replay be required by regulation to facilitate detection and proof of system failures); *see also infra* notes 300–02 and accompanying text (suggesting that the regulatory agency make adverse event reports available to the public).

177. *See infra* notes 331–32 and accompanying text (discussing financial incentives working against the adoption of interoperable EHR systems).

178. BIOMEDICAL INFORMATICS, *supra* note 1, at 451.

179. *See infra* note 184 and accompanying text (discussing the numerous EHR products certified for use by providers). In the word-processing area, Microsoft's Word has nearly achieved such a monopoly.

180. *See infra* notes 326–27 and accompanying text (discussing the complexity of medical information).

3. The Current Oversight System: CCHIT

To its credit, the HIT industry has engaged in an effort to self-regulate, particularly through the Certification Commission for Healthcare Information Technology ("CCHIT").[181] However, this initiative falls far short of providing comprehensive oversight for EHR systems. CCHIT, a private-sector organization, was created in 2004 and is composed of three HIT industry associations: the American Health Information Management Association; the Healthcare Information and Management Systems Society; and the National Alliance for Health Information Technology.[182] HHS awarded CCHIT a three-year contract in September 2005 with a mandate to develop certification criteria and an inspection procedure for EHR systems in the areas of office-based ambulatory care, inpatient care, and interoperability.[183] CCHIT has certified over fifty ambulatory care EHR systems and a dozen inpatient systems under its 2007 criteria.[184] Applicants must pay CCHIT for certification,[185] and ambulatory care products are certified for a period of two years,[186] during which CCHIT monitors product changes[187] and requires recertification for products that have been significantly modified.[188]

CCHIT, however, is an industry-run organization, and its certification criteria are vulnerable to criticism as being excessively favorable to vendors. There are several areas of concern. First, prior to product testing, applicants are able to access the criteria, testing scenarios, and test scripts on CCHIT's website.[189] Vendors, therefore, need not be prepared for unanticipated tests that might reveal flaws in the system that they did not encounter in practicing the testing scenarios. Second, all testing for clinical functionality, interoperability, and

181. CCHIT: Certification Commission for Healthcare Information Technology, http://www.cchit.org/about/ index.asp (last visited Dec. 19, 2008).

182. FAQ Frequently Asked Questions — CCHIT Certification Commission for Healthcare Information Technology, http://www.cchit.org/about/faq/general.asp#founding (last visited Dec. 19, 2008).

183. CCHIT, CERTIFICATION HANDBOOK 60 (2008) [hereinafter CERTIFICATION HANDBOOK], *available at* http://www.cchit.org/files/certification/08/Forms/CCHITCertified 08Handbook.pdf.

184. *See* CCHIT, CCHIT Certified Ambulatory EHR 2007, http://www.cchit.org/choose/ambulatory/2007/index.asp (last visited Dec. 19, 2008); CCHIT Certified Inpatient EHR 2007, http://www.cchit.org/choose/inpatient/2007/index.asp (last visited Dec. 19, 2008).

185. *See* CERTIFICATION HANDBOOK, *supra* note 183, at 66–67.

186. *Id.* at 45 ("The term for Ambulatory EHR Certification, as it relates to a specific product version, will be two (2) years from the Certification Date . . . .").

187. *See id.* at 44 (detailing penalties for discrepancies between the certified product and the product that a company is actually marketing).

188. *See id.* at 47–49 (describing CCHIT policies and procedures pertaining to product modifications).

189. *Id.* at 15 (urging applicants to prepare for their inspection date by reviewing the material carefully and practicing their demonstration of the test scripts).

security occurs during one day.[190] Consequently, inspectors do not observe the system operating over time and in a variety of usage environments. Third, the certification jury is composed of "three clinical experts, at least one of whom must be a practicing physician."[191] However, jurors cannot confer or deliberate during the demonstration or voting process,[192] so they cannot draw each others' attention to concerns or product shortcomings.

CCHIT's single day of testing is particularly troubling because experience indicates that it is unlikely to detect many significant reliability and safety problems. Though there are many examples, a series of incidents involving the Therac-25 radiation therapy machine vividly illustrates this point. Between 1985 and 1987 six patients died of massive radiation overdoses caused by software defects.[193] The machine had passed safety analysis in 1983, which did not include software testing, and it was not recalled until after the sixth incident in 1987.[194] Likewise, flaws in EHR systems may not be initially obvious but could cause life-threatening errors after a period of time. Such errors could include deleting or incorrectly recording information about patient allergies, lists of medications already prescribed to a patient, or electronic medication orders. Patients who receive incorrect medications or drug dosages may well suffer serious or fatal harm.

CCHIT published final 2008 criteria for ambulatory care EHR products.[195] These documents are substantial and cover many important areas. However, they also leave significant gaps. For example, they do not specify requirements concerning the reliability[196] or safety[197] of EHR systems.[198]

CCHIT, in fact, recognizes some of its own limitations. Its Certification Handbook states:

---

190. *See id.* at 25–27 (describing durations of testing procedures).

191. *Id.* at 28.

192. *Id.* at 29.

193. Nancy G. Leveson, & Clark S. Turner, *An Investigation of the Therac-25 Accidents*, 26 IEEE COMPUTER 18, 21 (1993).

194. *Id.* at 20–21.

195. CCHIT, AMBULATORY CERTIFICATION CRITERIA — FINAL CRITERIA (2008), *available at* http://www.cchit.org/files/certification/08/Ambulatory/CCHITCriteriaAMBULATORY08FINAL.pdf.

196. The reliability of a system is the probability that it will correctly deliver services over a given interval of use. IAN SOMMERVILLE, SOFTWARE ENGINEERING 48 (8th ed. 2007).

197. A system's safety is "a judgment of how likely it is that the system will cause damage to people or its environment." *Id.*

198. This is true despite the fact that Section 5.6 of the CCHIT 2008 Certification Handbook indicates that the following is an approved description of the CCHIT certification program: "[CCHIT's] inspection process is based on real-life medical scenarios designed to test products rigorously against the clinical documentation needs of providers and the quality and safety needs of healthcare consumers and payers." CERTIFICATION HANDBOOK, *supra* note 183, at 61.

> [O]ur criteria at this point can only represent broad, basic capabilities, and . . . these may prove insufficient for some practice specialties, or may be inappropriate or excessive for others; . . . our criteria do not assess product usability, implementation service, product maintenance, technical and application support; and other facts.[199]

Admittedly, EHR systems could be required to have almost endless capabilities. Determination of which capabilities should be required will necessitate careful deliberation and input from many interested parties, including physicians, patient representatives, public interest groups, and academic researchers.

B. Who Should Regulate?

If EHR systems are to be regulated, their regulation must be assigned to a particular agency. This Section considers several options. While the FDA might initially seem to be the appropriate regulatory agency, it is not the optimal choice, for reasons elaborated below. The Centers for Medicare & Medicaid Services ("CMS") would be a better alternative, as would a newly created agency tasked with oversight of health information technology in the U.S.

1. FDA Jurisdiction

As noted above, the FDA thus far has not taken the initiative to regulate EHR systems.[200] The FDA's authority to regulate devices extends to computer software that is "integral to . . . or closely connected with" any apparatus that delivers patient care, such as a CAT scanner or a respirator.[201] However, its authority to regulate EHR systems is much more dubious.

In 1989 draft guidance, the FDA declined to extend its regulatory authority to software that is "intended for use only in traditional 'library' functions, such as storage, retrieval, and dissemination of medical information — functions traditionally carried out through textbooks or journals."[202] The FDA also exempted software with

199. *Id.* at 40.

200. *See* Miller, *supra* note 148.

201. *See* Rosoff, *supra* note 142, at 121.

202. CTR. FOR DEVICES & RADIOLOGICAL HEALTH, FDA, FDA POLICY FOR THE REGULATION OF COMPUTER PRODUCTS 1 (proposed 1989) [hereinafter 1989 DRAFT FDA POLICY], *available at* http://www.fda.gov/cdrh/ode/351.pdf. The policy was never formally adopted, but the draft policy informed the FDA's approach to stand-alone software systems throughout the 1990s. *See* Randolph A. Miller & Reed M. Gardner, *Recommendations for Responsible Monitoring and Regulation of Clinical Software Systems*, 4 J. AM. MED. INFORMATICS ASS'N 442, 445–46 (1997).

"general accounting or communication" and educational functions.[203] Of particular significance is the draft policy's exemption of computer products, such as decision support systems, that involve "competent human intervention before any impact on human health occurs."[204] EHR systems serve library, accounting, and communication functions. Furthermore, unlike pacemakers or respirators that operate independently once they are connected to the body, EHR systems have no impact without human input and intervention. Consequently, they would appear to be excluded from active FDA regulation under this policy.

In a 1996 workshop, the FDA recognized the difficulties of determining what constitutes "competent human intervention," which in turn determines whether medical software should be regulated by the agency.[205] With respect to decision support, "competent human intervention" requires that users have the time, motivation, and ability to reflect upon and challenge computer-generated data and recommendations, which may not be true in the midst of surgery or in the intensive care unit.[206] In addition, medical software is often so complicated that users cannot analyze or understand its computations and, therefore, cannot exercise competent human intervention.[207] EHR system complexity, in fact, is likely to increase as more sophisticated functions, such as diagnostic algorithms based on machine learning,[208] are incorporated. Doctors who rely excessively on computer-generated diagnoses and treatment recommendations may fail to perceive that the algorithms did not account for certain conditions that are pertinent to their patients. By the same token, some doctors may unreasonably mistrust EHR system decision support, choosing to follow their intuition, rather than computerized recommendations, to the detriment of their patients. Consequently, "competent human intervention" cannot protect adequately against potentially harmful software defects, since most clinicians will not be able to determine whether these sophisticated tools have formulated the correct approach in a particular instance. The 1996 workshop called for reexamination of the FDA's criteria for regulatory exemptions relating to software,[209] an initiative that has not been pursued to date.

---

203. 1989 DRAFT FDA POLICY, *supra* note 202, at 1.

204. *Id.* at 3.

205. FDA & Nat'l Library of Med., Software Policy Workshop (Sept. 3–4, 1996) (unpublished workshop handouts), *available at* http://www.netreach.net/~wmanning/fdaswsem.htm#background.

206. *Id.*

207. *Id.*

208. "Machine learning" refers to a machine's ability to learn to perform tasks through examples or analogies to similar, previously-executed tasks and to improve performance based on past experience. Jaime G. Carbonell et al., *An Overview of Machine Learning*, *in* MACHINE LEARNING: AN ARTIFICIAL INTELLIGENCE APPROACH 4 (Ryszard S. Cichalski et al. eds., 1985); TOM M. MITCHELL, MACHINE LEARNING 1 (1997).

209. FDA & Nat'l Library of Med., *supra* note 205.

One option for regulating EHR systems is to include them explicitly within the FDA's jurisdiction. The FDA might effect such an extension of its jurisdiction by explicitly adopting an interpretive rule that reconstrues its statutory authority over devices to include EHR systems. However, the courts have resisted past efforts by the FDA to expand its authority to cover an area that it has not traditionally regulated. For example, in *FDA v. Brown & Williamson Tobacco Corp.*, the Supreme Court concluded that the Food, Drug, and Cosmetic Act ("FDCA") did not grant the FDA jurisdiction over tobacco products.[210] When it comes to EHR systems, the HIT industry, like the tobacco industry, could oppose FDA regulatory authority and turn to the courts for relief. Consequently, the extension of the FDA's authority to EHR systems may require a revision of the FDCA's definition of "device"[211] to make clear that EHR systems are covered. Statutory amendments, however, are often hindered by special interest lobbying and political, rather than public policy, concerns.[212]

Even if the FDA had jurisdiction over EHR systems, regulation by this agency may not be the optimal approach. The regulatory framework that the FDA is likely to apply to EHR systems would be inadequate for these patient management tools.

The FDA classifies devices into three categories based on the level of oversight deemed necessary to assure their safety and efficacy.[213] "Class I devices" do not sustain, support, or protect human life or health and do not present an unreasonable risk of human illness or injury.[214] These devices are subject only to the FDA's "general controls," such as those relating to misbranding or adulteration.[215] "Class II devices" are used to support or sustain human life but do not pose the highest risk of injury. Such devices are subject to additional "special controls" at the discretion of the Secretary of HHS.[216] "Class III devices" sustain, support, or protect human life or health or present an unreasonable risk of causing human illness or injury.[217] Class III devices are subject to all of the above controls as well as to premarket approval ("PMA") by the FDA.[218]

---

210. 529 U.S. 120, 159–60 (2000).

211. For the current definition, see 21 U.S.C.A. § 321(h) (West 1999 & Supp. 2008).

212. *See* ANTONIN SCALIA, A MATTER OF INTERPRETATION 34–35 (1997) (discussing the role of lobbyists and arguing that, because of their involvement, legislative history is not an appropriate tool for statutory interpretation); Joseph Tussman & Jacobus tenBroek, *The Equal Protection of the Laws*, 37 CAL. L. REV. 341, 350 (1949) ("Everything that emerges from the legislative forum is tainted by its journey through the lobby.").

213. 21 U.S.C.A. § 360c (West 1999 & Supp. 2008); *see* A PRACTICAL GUIDE TO FOOD AND DRUG LAW AND REGULATION 127–30 (Kenneth R. Piña & Wayne L. Pines eds., 2d ed. 2002) [hereinafter A PRACTICAL GUIDE].

214. 21 U.S.C.A. § 360c(a)(1)(A).

215. A PRACTICAL GUIDE, *supra* note 213, at 128.

216. 21 U.S.C.A. § 360c(a)(1)(B).

217. *Id.* § 360c(a)(1)(C).

218. *Id.*

The FDA, however, allows manufacturers to avoid the PMA process by showing that their new device is "substantially equivalent"[219] to a legally marketed predicate device.[220] In order to obtain a finding of substantial equivalence, applicants can submit what is known as a "510(k) application."[221] The FDA will grant a PMA exemption if it determines that the device at issue has the same intended use as the predicate device and the same technological characteristics or that the device is demonstrably as safe and effective as an already marketed device.[222] Furthermore, the HHS Secretary is statutorily required to design information requests so that they are minimally burdensome to 510(k) applicants.[223] Accordingly, the FDA requires clinical data for only a minority of 510(k) reviews.[224]

The 510(k) process has become so popular with manufacturers who wish to avoid the more onerous and lengthy PMA procedure that over seventy-five percent of medical devices are approved through this process.[225] The 2004 Center for Devices and Radiological Health ("CDRH") annual report shows a consistent ten-to-one ratio of approved 510(k) applications to approved PMA applications from fiscal years 1999 through 2004.[226] Moreover, according to one source that reviewed 510(k) applications in the early 1990s, CDRH generally rejected only two percent of the applications.[227]

In light of this approval framework, it is unlikely that EHR systems would receive adequate scrutiny by the FDA. First, because EHR systems do not directly sustain, support, or protect human life or health, they may well be deemed Class I devices, which receive minimal oversight. Second, even if they are categorized as Class III devices, after the FDA approves the first EHR system, subsequent

---

219. *Id.* § 360c(i).

220. *Id.* § 360c(f)(1); Benjamin A. Goldberger, *The Evolution of Substantial Equivalence in FDA's Premarket Review of Medical Devices*, 56 FOOD & DRUG L.J. 317, 318, 325–27 (2001) (discussing substantial equivalence).

221. Goldberger, *supra* note 220, at 318. The 510(k) application is named after the FDCA section that originally authorized the process, now codified at 21 U.S.C. § 360c(f)(1)(A). Eric Chan, Comment, *The Food and Drug Administration and the Future of the Brain-Computer Interface: Adapting FDA Device Law to the Challenges of Human-Machine Enhancement*, 25 J. MARSHALL J. COMPUTER & INFO. L. 117, 142 n.152 (2007).

222. 21 U.S.C.A. §§ 360c(f)(1), 360c(i)(1)(A).

223. *Id.* § 360c(i)(1)(D) ("[T]he Secretary shall consider the least burdensome means of demonstrating substantial equivalence and request information accordingly.").

224. Goldberger, *supra* note 220, at 329–30.

225. A PRACTICAL GUIDE, *supra* note 213, at 134.

226. CTR. FOR DEVICES & RADIOLOGICAL HEALTH, FDA, CDRH FISCAL YEAR 2004 ANNUAL REPORT 28 tbl.2 (2005), *available at* http://www.fda.gov/cdrh/annual/fy2004/fy2004.pdf (reporting that, in 2004, the CDRH approved 3917 new 510(k)s and 39 original PMAs).

227. STAFF OF SUBCOMM. ON OVERSIGHT & INVESTIGATION OF THE H. COMM. ON ENERGY & COMMERCE, 103D CONG., LESS THAN THE SUM OF ITS PARTS: REFORMS NEEDED IN THE ORGANIZATION, MANAGEMENT, AND RESOURCES OF THE FDA'S CENTER FOR DEVICES AND RADIOLOGICAL HEALTH 38 (Comm. Print 1993).

systems would probably be reviewed under the substantial equivalence standard rather than the more rigorous PMA standard.[228] Two EHR systems produced by different vendors, however, are likely to have very different programming, and hence their reliability may differ dramatically. Thus, the 510(k) process is ill-suited to the approval of new EHR systems and should not be the basis of EHR system regulation.

Finally, the FDA is currently a beleaguered entity. The FDA is subject to budgetary limitations that could constrain its ability to exercise adequate oversight over complicated technological devices.[229] The agency has also been heavily criticized for inadequacies in its approval and monitoring processes and for other shortcomings.[230]

2. Oversight by the Center for Medicare & Medicaid Services or a Newly Created Agency

The existing agency that might be best suited to regulate EHR systems is the Center for Medicare & Medicaid Services ("CMS"). According to CMS, as of 2002, 79.3 million individuals were CMS beneficiaries through Medicare, Medicaid, and the State Children's Health Insurance Program ("SCHIP"),[231] and providers earned approximately thirty-three percent of their revenues from the public programs overseen by CMS.[232] Essentially all hospitals and the overwhelming majority of physicians in the U.S. participate in Medicare, and many participate in Medicaid. Thus, they must follow CMS

228. *See* A PRACTICAL GUIDE, *supra* note 213, at 140–41 (comparing the 510(k) and PMA procedures).

229. Miller & Gardner, *supra* note 202, at 453.

230. *See, e.g.*, Russell Korobkin, *Who Should Protect the Public? The Supreme Court and Medical Device Regulation*, 357 NEW ENG. J. MED. 1680, 1680 (2007) ("[T]he FDA's post-approval monitoring system has been widely considered to be underfunded and hamstrung by the agency's limited authority."); Bruce M. Psaty & R. Alta Charo, *FDA Responds to Institute of Medicine Drug Safety Recommendations — In Part*, 297 JAMA 1917, 1917–19 (2007) (noting that the FDA is underfunded even though the products it regulates constitute 25% of the U.S. gross domestic product, that it suffers from a lack of transparency, that the agency relies on a "postmarketing surveillance system that could hardly be weaker," and that its post-approval enforcement mechanisms are often limited to threats of bad publicity); Sheila Weiss Smith, *Sidelining Safety — The FDA's Inadequate Response to the IOM*, 357 NEW ENG. J. MED. 960, 961 (2007) ("[T]he very structure of the FDA marginalizes safety."); Andrew Pollack, *New Sense of Caution at F.D.A.*, N.Y. TIMES, Sept. 29, 2006, at C1 (discussing the "barrage of criticism" aimed at the FDA).

231. CTRS. FOR MEDICARE & MEDICAID SERVS., PROGRAM INFORMATION ON MEDICARE, MEDICAID, SCHIP AND OTHER PROGRAMS OF THE CENTERS FOR MEDICARE & MEDICAID SERVICES: CMS PROGRAM OPERATIONS 3 (2002), http://www.cms.hhs.gov/TheChartSeries/downloads/sec2_z.zip.

232. CTRS. FOR MEDICARE & MEDICAID SERVS., PROGRAM INFORMATION ON MEDICARE, MEDICAID, SCHIP, AND OTHER PROGRAMS OF THE CENTERS FOR MEDICARE AND MEDICAID SERVICES: U.S. HEALTH CARE SYSTEM 6 (2002), http://www.cms.hhs.gov/TheChartSeries/downloads/sec1_z.zip.

mandates.[233] CMS has broad regulatory authority and has promulgated numerous federal regulations.[234] Consequently, assigning EHR system oversight to CMS would not subject most providers to regulation by an unfamiliar agency; rather, it would add to the requirements they must already meet in order to achieve CMS compliance. Furthermore, if enforcement provisions include the threat that violators would be denied Medicare, SCHIP, or Medicaid reimbursement, compliance is likely to be high.[235]

In order to extend CMS jurisdiction to the minority of providers that do not participate in any federal health care program, Congress would need to pass enabling legislation that would provide the agency with authority to regulate all EHR systems with respect to all patients, regardless of their Medicare, Medicaid, or SCHIP status. This approach would not be unprecedented, because CMS already enforces the HIPAA Security Rule,[236] which governs the security of electronic health information for a broad range of providers, regardless of whether they participate in Medicare, Medicaid, or SCHIP.[237] Furthermore, through its enforcement of the Security Rule, CMS has acquired expertise with respect to HIT.[238] Nevertheless, assigning CMS oversight responsibilities for EHR systems would require increases in the agency's human, financial, and other resources.

A second option, which has been suggested by HHS, is to create an entirely new regulatory agency that will be responsible for the development, implementation, and regulation of EHR systems and the NHIN.[239] Congress has periodically created new agencies to regulate emerging areas of law. For example, Title VII of the Civil Rights Act of 1964 established the Equal Employment Opportunity Commission,

---

233. Timothy Stoltzfus Jost, *Racial and Ethnic Disparities in Medicare: What the Department of Health and Human Services and the Centers for Medicare and Medicaid Services Can, and Should, Do*, 9 DEPAUL J. HEALTH CARE L. 667, 669 (2005) (describing Medicare participation); Sidney D. Watson, *Health Care in the Inner City: Asking the Right Question*, 71 N.C. L. REV. 1647, 1667 (1993) (stating that most hospitals participate in Medicaid).

234. *See, e.g.*, 42 C.F.R. pts. 400–413. (2007).

235. The HHS Secretary has authority to deny payment to skilled nursing facilities that have not met particular requirements. 42 U.S.C. § 1395i-3(h)(2)(B)(i) (2000). A similar penalty could be established for non-compliance with regulatory requirements pertaining to EHR Systems.

236. 45 C.F.R. §§ 160.302–.316 (2007).

237. *See* Centers for Medicare & Medicaid Services Statement of Organization, Functions, and Delegation of Authority, 68 Fed. Reg. 60,694, 60,694 (Oct. 23, 2003).

238. The Security Rule establishes administrative, physical, and technical requirements to safeguard the security of electronic health records. *See* 45 C.F.R. §§ 160.302–.316 (2007). CMS has authority to investigate and resolve claims of alleged Security Rule violations. 45 C.F.R. §§ 160.306, 160.308 (2007).

239. U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF NATIONWIDE HEALTH INFORMATION NETWORK (NHIN) REQUEST FOR INFORMATION (RFI) RESPONSES 12 (June 2005), http://www.hhs.gov/healthit/rfisummaryreport.pdf (suggesting that the federal government could create a health information agency to govern, finance, and set standards for the NHIN or could assign these tasks to an existing agency).

which enforces federal employment discrimination laws.[240] Under the Occupational Safety and Health Act of 1970, the Occupational Safety and Health Administration was established to promote workplace safety,[241] and the Health Care Financing Administration, now the Centers for Medicare & Medicaid Services, was established in 1977 to administer the Medicare and Medicaid programs.[242] Creation of a new agency may encounter resistance because it could be costly and would constitute an expansion of government. However, an adequately funded agency focused exclusively on HIT, with a concentration of technical talent and expertise, could be an effective vehicle for regulating EHR systems.

IV. RECOMMENDATIONS FOR A REGULATORY FRAMEWORK FOR EHR SYSTEMS

This Part develops recommendations for a regulatory framework to govern EHR systems. First, to achieve universal EHR system adoption, the government will need to provide financial support to resource-poor providers. The proposed regulations also address the design of approval and monitoring processes for EHR systems, standardization of essential system features and capabilities, and the creation of a national databank of de-identified EHRs. These recommendations aim to serve as a model that will initiate a discussion about the need for and potential contours of a regulatory scheme for HIT. They do not seek to perfect all of the details of future regulatory provisions.

A. Addressing the Cost of EHR System Adoption

1. Financial Support

As several legislators and administrative agencies have already recognized, it is unreasonable to expect widespread adoption of EHR systems without financial support.[243] The transition from paper files to EHR systems can be expensive, complicated, and burdensome, especially for smaller medical practices.[244] Given a regulatory requirement

240. The Civil Rights Act, 42 U.S.C. § 2000e-4 (2000); *see* U.S. Equal Employment Opportunity Commission (EEOC), http://www.eeoc.gov.

241. The Occupational Safety and Health Act, 29 U.S.C. §§ 651–78 (2006); *see* Occupational Safety and Health Administration — OSHA HOME PAGE, http://www.osha.gov.

242. CTRS. FOR MEDICARE & MEDICAID SERVS., KEY MILESTONES IN CMS PROGRAMS (2006), http://www.cms.hhs.gov/History/Downloads/CMSProgramKeyMilestones.pdf.

243. *See supra* notes 155–58 and accompanying text (discussing incentives for EHR system adoption).

244. *See supra* notes 131–38 and accompanying text (discussing the costs and burdens of EHR system implementation).

that all providers adopt EHR systems, the government should offer financial support in the form of tax credits, incentive payments, or grants to facilitate compliance.[245] As noted above, such inducements have already been suggested in several Congressional bills.[246]

According to many experts, governmental investments in HIT will be well worth their cost.[247] While the expenses of purchasing and implementing EHR systems will likely reduce net savings initially, savings are predicted to rise sharply once the systems have been fully implemented.[248] Assuming a base year of 2004, one study anticipated net national savings of $21.3 billion at year five, $59.2 billion at year ten, and $77.4 billion at year fifteen.[249]

A program of incentive payments or grants could be administered by the Agency for Healthcare Research and Quality ("AHRQ"), which is HHS's health research services arm.[250] One of the agency's functions is to serve as "a major source of funding and technical assistance for health services research and research training at leading U.S. universities and other institutions."[251] AHRQ, therefore, has considerable experience in administering grant programs[252] and has already provided funding for numerous HIT-related projects.[253]

2. WorldVistA

One approach that could alleviate funding pressures and facilitate development of an NHIN is widespread adoption of the VA's VistA system.[254] VistA is an open source product.[255] However, it is written in a programming language, MUMPS, that is currently unfamiliar to

245. *See* CONG. BUDGET OFFICE, *supra* note 80, at 27 (discussing the funding activities of the federal government and options for further promotion of HIT).

246. *See supra* notes 159–61 and accompanying text (discussing relevant legislative proposals).

247. *See, e.g.*, Hillestad et al., *supra* note 61, at 1115 (2005) ("[T]here is substantial rationale for government policy to facilitate widespread diffusion of interoperable HIT.").

248. *See id.* at 1114–15; Walker et al., *supra* note 80, at W5-16.

249. FEDERICO GIROSI ET AL., RAND HEALTH, EXTRAPOLATING EVIDENCE OF HEALTH INFORMATION TECHNOLOGY SAVINGS AND COSTS 35–36 (2005), *available at* http://www.rand.org/pubs/monographs/2005/RAND_MG410.pdf.

250. *See* What Is AHRQ?, http://www.ahrq.gov/about/whatis.htm (last visited Dec. 19, 2008).

251. *Id.*

252. *See* Health Care: Funding Announcements, http://www.ahrq.gov/fund/grantix.htm (last visited Dec. 19, 2008) (listing grant programs administered by AHRQ).

253. AHRQ National Resource Center for Health IT, http://healthit.ahrq.gov/portal/server.pt (last visited Dec. 19, 2008) (discussing AHRQ-funded state and regional HIT initiatives, e-prescribing pilot projects, and other undertakings).

254. *See* Goetz, *supra* note 131.

255. VistA Software Alliance, Vendors & Resources, http://www.vistasoftware.org/resources/index.html (last visited Dec. 19, 2008).

most programmers,[256] and it is not interoperable with other systems.[257] Furthermore, the VA does not offer assistance with installation and maintenance to those who adopt VistA, and therefore users must hire vendors for these purposes.[258]

In 2002, a group of VA programmers formed WorldVistA, which aims to extend and modify VistA for use outside the VA system and to assist users in mastering, installing, and maintaining the software.[259] The group received a grant from CMS to support its work.[260] In May 2007, a WorldVistA product for ambulatory care settings, WorldVistA EHR VOE/ 1.0, attained certification from CCHIT[261] and thus could be broadly adopted by physicians.[262]

Critics note that WorldVistA's staffing and billing functions are weak.[263] In addition, WorldVistA cannot be customized as easily as some other commercially available systems, and some feel its graphical interface is not particularly user-friendly or appealing.[264] While these shortcomings are significant, the cost of obtaining a license and support contract for WorldVistA is about ten percent of the cost of obtaining these items for other systems, according to one source.[265] However, the costs of installation, training, maintenance, and related activities may not be significantly lower.

The jury is still out as to whether the WorldVistA system can be sufficiently improved to become a broadly adopted, effective, and low cost alternative for health care providers. This option, however, is certainly worth exploring.

---

256. *See* Posting of Ignacio Valdes to LinuxMedNews, VistA and MUMPS: Big, Ugly and Proud, http://www.linuxmednews.com/1130420416/index_html (Oct. 27, 2005 08:40 EDT) ("MUMPS is also loathed by programmers . . . .").

257. Kupersmith et al., *supra* note 40, at w157–58 (describing the VA's EHR system); *The Last Frontier: Bringing the IT Revolution to Healthcare: Hearing Before the H. Comm. on Government Reform*, 109th Cong. 40, 46 (2005), (statement of Robert M. Kolodner, M.D., Chief Health Informatics Officer, Veterans Health Administration, Department of Veterans Affairs), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:24713.pdf ("Without data standards, we might be able to exchange health information, as we do now when we copy and send paper records, but we won't be able to use it as effectively to deliver safer, higher-quality care . . . . True interoperability between providers simply cannot be achieved without data standardization.").

258. *See* VistA Software Alliance, Vendors & Resources, *supra* note 255 (listing VistA service providers); *see also* Goetz, *supra* note 131 (stating that the VA is prohibited by law from straying from its mission to serve veterans and, consequently, it will not assist entities in installing or maintaining the system).

259. *See* Goetz, *supra* note 131; Welcome to the WorldVistA Homepage, http://worldvista.org (last visited Dec. 19, 2008); About WorldVistA, http://worldvista.org/WorldVistA (last visited Dec. 19, 2008).

260. Goetz, *supra* note 131.

261. See *supra* Part III.A.3 for detailed discussion of CCHIT.

262. WorldVistA EHR — CCHIT Certification Commission for Healthcare Information Technology, http://www.cchit.org/choose/ambulatory/2006/WorldVistA-EHR.asp (last visited Dec. 19, 2008).

263. *See, e.g.*, Goetz, *supra* note 131.

264. *Id.*

265. *Id.*

B. Regulating Approval and Oversight of EHR Systems

CCHIT has promoted EHR system quality by developing certification criteria and certifying ambulatory care and hospital EHR products through its testing program.[266] Without CCHIT, EHR systems would not be subject to oversight of any kind.[267] However, assigning certification of EHR systems exclusively to CCHIT, an industry-based association, is inadequate. Instead, we recommend that federal regulations establish a multi-step process that will involve scrutiny by a variety of parties. Regulatory requirements should apply to all parties who develop or modify EHR system software, install it, or integrate it with existing systems. Health care providers who perform these functions themselves should be deemed vendors for legal purposes relating to EHR system activities ordinarily performed by vendors.

The essential components of our recommendations are the following: (1) field testing of all new products for a significant period of time; (2) use of local EHR System Oversight Committees that will in some ways resemble Institutional Review Boards ("IRBs");[268] (3) premarketing product approval by the regulatory agency; and (4) ongoing, post-marketing monitoring by the Committees and the regulating agency to ensure that adverse event data is collected, that vendors respond to users' requests for assistance, and that system failures are promptly investigated and addressed so that adverse health outcomes are avoided or minimized. These elements are developed below.

1. Initial Approval of New Products

New EHR systems should not be available for use without approval by the regulatory agency. To begin the approval process, applicants seeking EHR system approval would submit to the regulating agency[269] the following items: project plans; software requirements and specifications; software designs; test plans; test reports; documentation for users and system administrators; and related documents. The material should include guidelines concerning how and to what extent health care providers can safely customize the product, together with a technical justification for why the permissible customizations are considered safe.

Actual testing of the system would commence with "in house" testing by the system developer. In addition, developers may choose to retain CCHIT to conduct the one-day testing program that it cur-

266. *See* CCHIT: Certification Commission for Healthcare Information Technology, http://www.cchit.org/certify/index.asp (providing information about CCHIT certification).

267. *See supra* notes 200–04 (explaining that the FDA does not regulate EHR systems).

268. *See* 21 C.F.R. § 56.102(g) (2007) (defining "Institutional Review Board").

269. See *supra* Part III.B for discussion of which agency should have regulatory authority.

rently offers,[270] though they would not be required to do so. CCHIT review might be useful because it could alert developers to problems that they had not detected through internal testing prior to launching their products for pilot testing in the field.

Prior to approval, EHR systems would be field tested for a period of at least six months under varied and representative usage conditions.[271] Such testing is needed because the occurrence of software failures may be highly dependent on the local operating environment and patterns of usage.[272] The FDA recognizes the need to test software in medical devices at the user site.[273] CCHIT has also recognized the need for systems to be observed in the field. It requires that they be in operation at one or more locations for forty-five days prior to testing.[274] This requirement, however, is not sufficiently rigorous, because such a limited evaluation does not account for variations in function usage across sites or over time. Indeed, within the first forty-five days, users may not even become thoroughly familiar with a system or use all of its functions.[275] We recommend that systems designed for hospitals be tested at a small number of medium to large hospitals and that systems designed for ambulatory care settings be tested in a larger number of provider offices.

The regulating agency should publish site-selection and testing-period guidelines and evaluation metrics for different types of EHR systems. The guidelines should be based upon sound survey methodology[276] so as to ensure that meaningful statistical estimates of adverse incident frequency, software reliability,[277] and other relevant measures are obtained.

---

270. *See supra* notes 189–94 and accompanying text (discussing the CCHIT testing program).

271. *See* Richards, *supra* note 20, at 27 (discussing the importance of creating "a real-world test environment").

272. John Musa et al., *The Operational Profile*, *in* HANDBOOK OF SOFTWARE RELIABILITY AND SYSTEM RELIABILITY 167, 167 (Michael R. Lyu ed., 1996) ("A software-based product's reliability depends on just how a customer will use it.").

273. FDA, GENERAL PRINCIPLES OF SOFTWARE VALIDATION; FINAL GUIDANCE FOR INDUSTRY AND FDA STAFF 27 (2002), *available at* http://www.fda.gov/cdrh/comp/guidance/938.pdf.

274. CERTIFICATION HANDBOOK, *supra* note 183, at 45 (requiring that products be in production use for forty-five calendar days in at least one location).

275. *See* Linda M. Culp et al., *Phased Implementation*, *in* IMPLEMENTING AN EHR SYSTEM, *supra* note 20, at 111, 111 (discussing the importance of spreading "the users' learning over time" and "producing several manageable peaks in cognitive load").

276. *See generally* RISTO LEHTONEN & ERKKI PAHKINEN, PRACTICAL METHODS FOR DESIGN AND ANALYSIS OF COMPLEX SURVEYS (2004).

277. *See* SOMMERVILLE, *supra* note 196, at 208–09, 801 (explaining that reliability metrics are used to specify software reliability, that is, the system's ability to "deliver services as specified").

2. The Role of Local System Oversight Committees

Effective approval and monitoring of all EHR systems in the U.S. could not be accomplished solely by the regulatory agency. Rather, it will have to be led by local entities that are sufficiently resourced to achieve thorough and constant oversight. We will call these entities EHR System Oversight Committees ("SOCs"), and we contemplate that they will be similar in some ways to IRBs.[278] The use of SOCs for oversight of clinical software systems of various kinds was proposed a decade ago in an article written by two medical informatics experts, Randolph Miller and Reed Gardner,[279] and several of our recommendations overlap with theirs.[280]

Hospitals and physician networks with sufficient IT resources would have their own SOCs. Local SOCs would also be created to serve resource-poor hospitals or individual providers' offices that wish to join together for SOC purposes.[281] Just as federal regulations govern the composition of IRBs,[282] regulations would specify guidelines for the number, expertise, and diversity of SOC members.

Vendors would need to convince provider facilities to agree to field test new EHR systems. Participating providers would have to enter existing patient records into the EHR system that is to be tested, which can be an onerous task; therefore, vendors would likely find it necessary to offer significant incentives.[283] Providers might be willing to serve as field testers only if they are convinced that the product is superior to others that have already been approved or is equivalent to others but is less expensive. To this end, a positive evaluation from CCHIT based on its one-day testing process[284] might be influential. Furthermore, vendors could offer field testers product discounts, free support services, and other payments or benefits, and they could promise that, in the event their product is not ultimately approved by

278. *See* Sharona Hoffman, *Regulating Clinical Research: Informed Consent, Privacy, and IRBs*, 31 CAP. U. L. REV. 71, 76–78 (2003) (discussing IRBs and their functioning).

279. *See* Miller & Gardner, *supra* note 202, at 450 (recommending review of clinical software systems by Software Oversight Committees, composed of individuals with expertise in "health care informatics, clinical practice, data quality, biomedical ethics, patients' perspectives, and quality improvement").

280. See the footnotes in this Part for references to relevant proposals in the Miller & Gardner article.

281. *See* Miller & Gardner, *supra* note 202, at 450 (suggesting that small practitioners' offices and hospitals could "participate in regional SOCs, or possibly request consultations from local SOCs at larger institutions").

282. 21 C.F.R. § 56.107 (2007) (discussing IRB membership).

283. In some cases, facilities may be allowed to test EHR systems using a subset of their patient records rather than all of them. The regulatory agency will need to develop guidelines as to how many records must be included in order to obtain statistically significant field testing results.

284. *See supra* notes 189–92 and accompanying text (discussing the CCHIT testing program).

the regulating agency, they will provide reimbursement for expenses incurred in testing the system.

SOCs would charge vendors a review fee, but this would not constitute a novel or unacceptable requirement. CCHIT charges a fee,[285] as do IRBs that operate for profit and bill for protocol reviews.[286] Drug and device manufacturers seeking FDA approval have also become accustomed to paying the FDA user fees pursuant to the Prescription Drug User Fee Act[287] and the Medical Device User Fee and Modernization Act of 2002.[288] Furthermore, the FDA at times relies on paid third party reviewers during the device approval process. In some circumstances, device manufacturers may request that their facility inspection be conducted by an "accredited person" rather than by an FDA official.[289]

Despite being paid a fee by vendors, SOCs are more likely to be neutral than CCHIT, because most of their members would not be HIT industry personnel. Rather, their membership would include hospital HIT staff, physicians and other health care workers, community members representing patients, academics, and others. These individuals are likely to prioritize the best interests of practitioners and patients over the interests of industry and thus to subject EHR systems to rigorous evaluation.

The SOCs would oversee testing, review field testing results, and produce a report evaluating the EHR system upon completion of testing. The EHR system vendor would then submit required documentation, including the SOC's report, to the regulatory agency, which would have ultimate approval authority.[290]

While this multi-step process may seem onerous, it is no more burdensome than the traditional FDA approval process for new drugs. The FDA approval process entails animal testing, human testing in three separate phases of clinical trials, review of safety and efficacy research by an FDA review team, FDA review of labeling informa-

---

285. *See* CERTIFICATION HANDBOOK, *supra* note 183, at 66 (detailing fees for CCHIT testing).

286. *See* Sharona Hoffman & Jessica Wilen Berg, *The Suitability of IRB Liability*, 67 U. PITT. L. REV. 365, 404 (2005) (discussing for-profit IRBs).

287. 21 U.S.C.A. § 379h (West 1999 & Supp. 2008) (detailing fees that those submitting human drug applications must pay).

288. *Id.* § 379j(a) (detailing fees that those submitting PMAs must pay).

289. *See id.* § 360m (authorizing review by accredited persons); *see also* Accredited Persons Inspection Program, http://www.fda.gov/cdrh/ap-inspection/ap-inspection.html (last visited Dec. 19, 2008) (describing the program and its operation). An "accredited person" is one who is certified through an accreditation program to conduct certain review functions. The qualifications for accredited persons are listed in 21 U.S.C.A. § 360m(b)(3).

290. *See* 21 C.F.R. §§ 814.20, 814.40 (2007) (discussing items that must be included in submissions for pre-market approval and the FDA's authority to approve and disapprove these submissions).

tion, and an FDA facility inspection.[291] EHR systems, which are vital to patient health and welfare, must similarly be subjected to rigorous review.[292]

EHR systems that are already CCHIT-certified[293] and are in use at the time the regulations go into effect would not need to be approved by the regulating agency. It would be unrealistic and excessively disruptive to require providers to suspend use of EHR systems upon which they already depend in order to subject them to lengthy approval processes. If such demands were made, physicians would have to return temporarily to using paper records and might lose access to critical medical history and other information about their patients. Systems that are already in use would be subjected to the reporting and monitoring requirements outlined below,[294] which should be sufficient to detect any product flaws that require corrective intervention.

3. The Need for Continued Monitoring

The operating conditions that an EHR system encounters when it is broadly deployed may differ from those it encountered during field testing. Furthermore, the system itself may be changed by the vendor or by users, for example, to fix defects, add new features, or accommodate local preferences. Therefore, system monitoring should continue for the operational lifetime of the product.

To facilitate timely recognition of and response to emerging problems, EHR system vendors would be required to provide several mechanisms by which users can report difficulties. These would include a feature that is incorporated into the EHR system itself, such as a button labeled "Report System Problem," a vendor website through which problem reports can be submitted, and a dedicated e-mail address and phone number for reporting problems.[295]

EHR vendors would notify the SOCs overseeing affected facilities of all problems and categorize problems in terms of severity and potential impact on patients and providers.[296] Early in the process of EHR system implementation, it is likely that a large percentage of

---

291. Michelle Meadows, *The FDA's Drug Review Process: Ensuring Drugs Are Safe and Effective*, FDA CONSUMER MAGAZINE, July/Aug. 2002, at 19, 21, *available at* http://www.fda.gov/fdac/special/testtubetopatient/drugreview.html.

292. As technology develops, some safety-critical components of EHR system decision support, such as diagnostic algorithms designed to detect various cancers, may need to be separately evaluated. In such cases, traditional clinical trials may be appropriate, and these could be referred to the FDA or overseen by the agency that regulates EHR systems.

293. *See* CERTIFICATION HANDBOOK, *supra* note 183, at 8 (noting that over 100 products have been certified by CCHIT).

294. *See infra* Part IV.B.3 (discussing continued monitoring of EHR systems).

295. *Cf.* Elizabeth A. Boyer & Michael W. Soback, *Production Support*, *in* IMPLEMENTING AN EHR SYSTEM, *supra* note 20, at 95, 95 (discussing how an EHR help desk should operate).

296. *See id.* at 96 (describing a methodology for classifying and tracking problems).

problems will be minor ones, resulting from users' lack of familiarity with the system. Once problems are resolved, vendors would notify SOCs and explain the resolutions. As a safeguard against vendors concealing problems, users could also be encouraged to report significant problems directly to their SOCs through SOC websites or e-mail.[297]

All SOCs, in turn, would provide the regulatory agency with semi-annual reports of significant EHR system problems, their resolutions, and accounts of vendors' failures to address serious problems.[298] However, SOCs and vendors would immediately report to the regulating agency any serious problems that might endanger the health of patients so that the agency can oversee the remediation process and, if necessary, investigate and impose appropriate penalties. The FDA has established similar adverse event reporting requirements for user facilities, importers, and manufacturers of devices.[299]

The regulatory agency should post confirmed problem reports on its website so that consumers who are considering purchasing new EHR systems can evaluate them in light of all available information.[300] The reports should, however, delete trade secret information, confidential commercial and financial information, patient information, and information about the identities of the users who reported the adverse events.[301] This practice would follow the precedent established by the FDA, which has the authority to disclose redacted adverse event reports for medical devices.[302]

Software vendors routinely modify their systems to repair defects and add new features.[303] Any change to existing software, including EHR system software, creates the possibility of operational failures due to newly introduced defects.[304] The FDA has indicated that 7.7%

---

297. *See* Miller & Gardner, *supra* note 202, at 450–51 (stating that SOCs should monitor user complaints and ensure that vendors provide users with a help desk and correct software problems); *see also* CERTIFICATION HANDBOOK, *supra* note 183, at 43 (discussing CCHIT's "Purchaser Complaint Process").

298. *See* Miller & Gardner, *supra* note 202, at 451 (suggesting that SOCs should report product problems to the FDA).

299. 21 C.F.R. § 803.1 (2007).

300. *See* Miller & Gardner, *supra* note 202, at 451 (recommending that the FDA "collect and distribute aggregated, standardized reports of system-specific and global problems").

301. *Cf.* 21 C.F.R. § 803.9 (discussing public disclosure of medical device reports).

302. *Id.* §§ 803.9, 814.44(d); *see* Aaron Kesselheim & Michelle Mello, *Confidentiality Laws and Secrecy in Medical Research: Improving Public Access to Data on Drug Safety*, 26 HEALTH AFF. 483, 489–90 (2007) (calling for regulatory and legislative changes that would require the FDA to expand its disclosure of safety data so that researchers can independently assess drug safety and efficacy).

303. *See* SOMMERVILLE, *supra* note 196, at 488–511 (discussing software evolution).

304. *See* Elizabeth Boyer et al., *System Integration*, *in* IMPLEMENTING AN EHR SYSTEM, *supra* note 20, at 89, 94 ("[M]ajor upgrades can create enough data integrity and usability problems to pose a serious threat to patient safety and workflow efficiency."); Nayar & Miller, *supra* note 112, at 48 (discussing various changes that can threaten the integrity of EHRs).

of medical device recalls between 1992 and 1998 were attributable to software failures, and among these, 79% of recalls were due to defects introduced by changes made after the software was initially produced and distributed.[305]

Vendors would report proposed system modifications to the SOCs that field tested their products with a good faith assessment of their potential impact on providers and patients.[306] SOCs would have authority to approve minor changes but would report major changes to the regulatory agency, which in turn could require a new approval process, including field testing.[307]

Vendors are not the only parties that might alter EHR systems. Health care providers themselves often customize the systems they use, for example, to accommodate their preferred workflows.[308] While many customizations entail little risk, others, such as customizing decision support rules, can impact patient welfare.[309] Health care providers who wish to make configuration changes or customizations to EHR systems that do not conform to approved customization guidelines[310] or that directly impact patient safety would report their proposed alterations to their SOCs. The SOCs would scrutinize the proposals to determine their potential impact on patient care and approve or disapprove them. While both SOCs and the regulatory agency would oversee significant system changes made by vendors,[311] the SOCs alone can oversee configuration changes and customizations made by health care providers.

The need to monitor technologically sophisticated devices has been acknowledged by industry and government. CCHIT has recognized the need for periodic recertification of products.[312] Likewise,

---

305. FDA, *supra* note 273, at 3.

306. *See* CERTIFICATION HANDBOOK, *supra* note 183, at 47–49 (discussing how CCHIT addresses minor and significant product changes). EHR systems should be designed so that changes to the system configuration can be made only by authorized system administrators and not by ordinary users. This constraint should apply even to seemingly minor user-interface changes, such as moving windows, because such changes could obscure clinically relevant information.

307. *See id.* Changes designed to fix system bugs, however, should be deployed before they are approved by an SOC or the regulatory agency.

308. *See* Jean A. Adams et al., *Workflow Assessment and Redesign*, *in* IMPLEMENTING AN EHR SYSTEM, *supra* note 20, at 36, 36–39 (discussing tailoring workflows for particular organizations).

309. For example, alerts and reminders that appear at the wrong time during the treatment encounter might fail to influence care decisions and improve health outcomes. *See* James M. Walker & Stephen T. Tingley, *Clinical Decision Support*, *in* IMPLEMENTING AN EHR SYSTEM, *supra* note 20, at 67, 70 ("If the reminder can only be presented after the physician has decided on a course of action and recommended it to the patient, it is likely to be ignored.").

310. *See supra* Part IV.B.1 (discussing customization features and their approval).

311. *See* Boyer et al., *supra* note 304, at 93–94 (advocating a "structured approach" to large system upgrades).

312. CERTIFICATION HANDBOOK, *supra* note 183, at 3.

Congress has authorized the Secretary of HHS to order post-marketing studies of devices whose malfunctions could lead to "serious adverse health consequences."[313] EHR systems are life-critical devices that demand similar attention.

Finally, the regulatory agency could maintain a feature on its website by which users can post comments concerning EHR systems that regulators will consider for purposes of future policy setting. HHS and CMS already maintain interactive sites that allow the public to submit questions and feedback.[314]

While the proposed regulatory scheme may appear to entail the creation of a large and costly government bureaucracy, this need not be the case. CCHIT certified fewer than sixty-five products under its 2007 criteria.[315] Thus, the number of EHR systems for which approval is sought at any given time is likely to be limited. In addition, if more stringent approval and monitoring requirements are implemented, vendors may be even more cautious and selective in attempting to introduce new products to the market.

C. EHR System Standards and Criteria

Regulators with specialized expertise will need to formulate the regulations carefully, in light of input received from various stakeholders through the statutorily mandated notice and comment period.[316] The agency will also likely find it necessary to periodically augment and revise the regulations and issue interpretive guidance to respond to the rapid pace of technological change. In this Section, we highlight only a few standards and requirements that deserve special emphasis and explanation.

1. Best Practices Standard

The task of crafting clear guidance concerning health information technology, software engineering methodology, and computer security practices is particularly challenging. These domains are continu-

313. 21 U.S.C.A. § 360*l* (West 1999 & 2008).

314. Submit Feedback: Centers for Medicare & Medicaid Services, http://questions.cms.hhs.gov/cgi-bin/cmshhs.cfg/php/enduser/ask.php (last visited Dec. 19, 2008); United States Department of Health & Human Services, Office for Civil Rights, http://www.hhs.gov/ocr/contact.html (last visited Dec. 19, 2008).

315. *See* CCHIT Certified Ambulatory EHR 2007, http://www.cchit.org/choose/ambulatory/2007/index.asp (last visited Dec. 19, 2008); CCHIT Certified Inpatient EHR 2007, http://www.cchit.org/choose/inpatient/ 2007/index.asp (last visited Dec. 19, 2008).

316. *See* 5 U.S.C. § 553(b)–(c) (2006) (establishing notice and comment requirements for proposed administrative rules). Initially, regulators may need to solicit input from industry members who are unfamiliar with the regulatory process. To this end, regulators may want to take advantage of eRulemaking initiatives, which allow the public to access and comment upon proposed federal regulations through the Internet. *See* Regulations.gov, http://www.regulations.gov/search/about.jsp (last visited Dec. 19, 2008).

ally changing, and thus it is very difficult to create static rules to govern them.[317]

Consequently, we recommend the adoption of a "best practices" standard. Specifically, the regulations should require EHR system vendors and health care providers to make reasonable efforts to identify and employ best practices relating to all of the following: hazard and risk analysis and mitigation; software development, validation, and maintenance; security measures; and system integration and operation. The practices identified should be either commonly used by organizations doing similar work or clearly superior to best common practices. The best practices standard is intended to motivate EHR system vendors to continually maximize the dependability of their products.

Vendors and health care providers could refer to consensus guidelines formulated by well respected professional organizations, such as the International Organization for Standardization ("ISO"),[318] or they could refer to HIT and software engineering publications. Regulators may choose to incorporate certain consensus guidelines by explicit reference in the regulations. In addition, on its website, the regulating agency could maintain a list of resources from which vendors and health care providers could draw guidance concerning best practices.

2. Interoperability

The federal regulations must address interoperability because it is essential to fully realizing the potential benefits of EHR systems for both clinical operations and medical research.[319]

Efforts to achieve HIT interoperability have been underway for many years. For example, in 1987, an ad hoc standards group called Health Level 7 ("HL7") was established to provide a standard for the exchange of information among hospital computer systems.[320] Now HL7 has in excess of 500 organizational members and 2200 individual members, and its data messaging standard is in use at over 1500 medical facilities.[321] Yet, despite HL7 and a number of other long-

317. *See* Hoffman & Podgurski, *supra* note 115, at 11.

318. ISO — International Organization for Standardization, http://www.iso.org/iso/home.htm (last visited Dec. 19, 2008).

319. *See supra* Part II.B.1 (discussing the importance of interoperability); *see also* Marco Eichelberg et al., *A Survey and Analysis of Electronic Healthcare Record Standards*, 37 ACM COMPUTING SURVS. 277, 278 (2005) ("Making EHRs interoperable will contribute to more effective and efficient patient care by facilitating the retrieval and processing of clinical information about a patient from different sites [among other benefits]."); Sebastian Garde et al., *Towards Semantic Interoperability for Electronic Health Records: Domain Knowledge Governance for openEHR Archetypes*, 46 METHODS INFO. MED. 332, 340–41 (2007) (discussing the importance of interoperability).

320. BIOMEDICAL INFORMATICS, *supra* note 1, at 300.

321. *Id.* at 301.

term efforts to achieve full interoperability of health information systems,[322] progress has been slow.[323]

The most relevant form of interoperability for our purposes is *semantic* interoperability, by which we mean "the ability of information systems to exchange information on the basis of shared, pre-established and negotiated meanings of terms and expressions."[324] In the context of EHR systems, this definition implies that all or part of an EHR created or updated on one system can be transmitted to other vendors' systems in a way that permits the receiving systems to interpret and utilize the transmitted data as efficiently and effectively as they use their own internally created EHRs.[325]

One obstacle to achieving semantic interoperability between EHR systems is the fact that medical terminology is complex, variable, and evolving. Terminology varies between medical specialties, locales, and health care facilities, and it also varies with clinical context.[326] For example, the abbreviation "MS" stands for "mitral stenosis" in cardiology, "multiple sclerosis" in neurology, "morphine sulfate" in anesthesia, and "magnesium sulfate" in obstetrics.[327] EHR systems that use different medical terminologies cannot communicate effectively with each other without an accurate translation between their terminologies.

Another barrier to achieving semantic interoperability is the fact that existing EHR systems produced by different vendors employ proprietary internal representations of medical information that are gen-

---

322. *See* Eichelberg et al., *supra* note 319, at 278 (discussing various standards that are being developed to address EHR interoperability problems).

323. B.G.M.E. Blobel et al., *Semantic Interoperability: HL7 Version 3 Compared to Advanced Architecture Standards*, 45 METHODS INFO. MED. 343, 345 (2006) (acknowledging the lengthy evolution of HL7, characterized by a "frequent change of direction" and an "endless series of versions," but expressing optimism that HL7 is a maturing standard that is steadily improving); *see* Barry Smith & Werner Ceusters, *HL7 RIM: An Incoherent Standard*, 124 STUD. HEALTH TECH. & INFORMATICS 133, 133–38 (2006) ("[A]fter ten years of effort, and considerable investment . . . , the promised benefits of interoperability remain elusive[.]").

324. Kim H. Veltman, *Syntactic and Semantic Interoperability: New Approaches to Knowledge and the Semantic Web*, 7 NEW REV. INFO. NETWORKING 159, 167 (2001).

325. This is the type of interoperability sought by HL7, one of whose core strategies is to "[d]evelop coherent, extendible standards that permit structured, encoded health care information of the type required to support patient care, to be exchanged between computer applications while preserving meaning." About HL7, http://www.hl7.org/about/hl7about.htm (last visited Dec. 19, 2008). Simply converting an EHR to human-readable text and transmitting it to another system does not constitute semantic interoperability if the receiving system cannot automatically distinguish the elements of the EHR, such as symptoms, test results, diagnoses, and drug orders, and process them appropriately.

326. Some commentators argue that the development and maintenance of a semantically interoperable representation for health information needs to be coordinated internationally and across health disciplines, a process that has been called "domain knowledge governance." *See* Garde et al., *supra* note 319, at 336–38.

327. Christopher G. Chute, *Medical Concept Representation*, *in* MEDICAL INFORMATICS: KNOWLEDGE MANAGEMENT AND DATA MINING IN BIOMEDICINE 170 tbl.6-1 (Hsinchun Chen et al. eds., 2005).

erally incompatible with one another.[328] To address this problem, it is necessary for all vendors to support what we will call a "common exchange representation" ("CER") for EHRs. A CER is an artificial language for representing the information in EHRs, which has well defined syntax and semantics and is capable of unambiguously representing the information in any EHR from a typical EHR system. EHRs using the CER should be readily transmittable between EHR systems of different vendors. The CER should make it easy for vendors of EHR systems to implement a mechanism for translating accurately and efficiently between the CER and the system's internal EHR format.[329] A CER should be based on a standardized clinical terminology such as SNOMED-CT.[330]

Financial disincentives constitute a further impediment to interoperability. Interoperability may be disfavored by providers because it makes it easier for patients to change doctors by allowing complete patient files to be shared or transferred electronically to other facilities.[331] Additionally, clinicians may be resistant to facilitating the sharing of patient data because they are sensitive to confidentiality issues and will worry that electronically transmitted EHRs will be accessed by unauthorized personnel or inadvertently distributed to persons with whom they should not be shared.[332] At the same time, some providers may be concerned that other clinicians who scrutinize their EHRs may accuse them of malpractice.

EHR system vendors may also find interoperability unappealing because it makes it easier for providers who have one EHR system to switch to another by enabling patient EHRs to be easily transferred

---

328. *See, e.g.*, Rong Chen et al., *Julius — A Template Based Supplementary Electronic Health Record System*, 7 BMC MED. INFORMATICS & DECISION MAKING (2007), http://www.biomedcentral.com/content/pdf/1472-6947-7-10.pdf (discussing attempts to combine EHR systems in three facilities in Stockholm, Sweden that encountered this problem).

329. *See* Marco Eichelberg et al., *Electronic Health Record Standards — A Brief Overview*, 2006 ITI 4TH INT'L CONF. ON INFO. & COMM. TECH., *available at* http://www.srdc.metu.edu.tr/webpage/projects/ride/publications/icict06_20060810.pdf (discussing EHR standards that would enable information exchange). An example of a proposed exchange representation for medical information is the HL7 Clinical Document Architecture ("CDA"). *See* Robert H. Dolin et al., *The HL7 Clinical Document Architecture*, 8 J. AM. MED. INFORMATICS ASS'N 552, 552–69 (2001).

330. *See* IHTSDO: International Health Terminology Standards Development Organisation, http://www.ihtsdo.org/ (last visited Dec. 19, 2008); *see also* PRESIDENT'S INFO. TECH. ADVISORY COMM., REVOLUTIONIZING HEALTH CARE THROUGH INFORMATION TECHNOLOGY 21–22 (2004), *available at* http://www.itrd.gov/pitac/reports/20040721_hit_report.pdf (recommending that SNOMED-CT be incorporated into EHR systems).

331. David J. Brailer, *Interoperability: The Key to the Future Health Care System*, 25 HEALTH AFF. W5-19, W5-20 (2005), (noting that without interoperability a health care enterprise "hopes to gain comparative advantage by imposing high costs on consumer switchover and by exercising market leverage over small-niche players such as solo physicians and community hospitals").

332. *See* 45 C.F.R. §§ 160.101–.534 (2007) (emphasizing the importance of the privacy and security of health information).

between systems. Without interoperability, the difficulty of transferring hundreds or thousand of EHRs between different systems may deter providers from changing their EHR vendors.

Although HIT has been developing over several decades, interoperability is an elusive goal, and the industry has seen a proliferation of non-interoperable products.[333] Today, we are far from achieving a fully interoperable NHIN.[334] According to some commentators, "the strategy of building the network from the bottom up by establishing many RHIOs throughout the country is not working."[335] Because of funding shortages, only a handful of RHIOs are fully operational and self-sustaining.[336] The only mechanism that is likely to achieve true nationwide interoperability, other than a monopoly of the EHR market, is a federal mandate that any EHR system that is approved for clinical use must support a specified CER.[337]

3. Audit Trails and Capture/Replay

Because EHR systems are extremely complex, regulators and litigants might find it impossible to discern certain system malfunctions without audit trails or capture/replay, even if they employ knowledgeable experts. A computer system audit trail is a "generalized recording of 'who did what to whom, when, and in what sequence.'"[338] It is also possible to design software to capture its interaction with users or with another system in such a way that the interaction can be replayed exactly as it happened, including graphical, as opposed to only textual, output.[339] Requiring either mechanism for EHR systems would be analogous to the HIPAA Security Rule's requirement of audit controls for systems that process electronic health information[340] and to the

333. *See supra* text accompanying notes 177–80 (discussing obstacles to interoperability).

334. *See* Day, *supra* note 35, at 1011 (explaining that "very few systems today are interoperable" and that EHR exchanges will be limited to local and regional RHIOs rather than to an NHIN for "some time to come").

335. CASTRO, *supra* note 57, at 10.

336. *See id.*; Julia Adler-Millstein et al., *The State of Regional Health Information Organizations: Current Activities and Financing*, 27 HEALTH AFF. w60, w63, w65–w66 (reporting on a survey of 138 RHIOs that found that 26% were defunct, "only twenty were functioning at even a modest scale, and only fifteen were doing so for a broad set of patients").

337. *See* PRESIDENT'S INFO. TECH. ADVISORY COMM., *supra* note 330, at 24–25 (discussing the importance of developing "a single set of data standards for the most common forms of clinical information").

338. Lawrence A. Bjork, Jr., *Generalized Audit Trail Requirements and Concepts for Data Base Applications*, 14 IBM SYS. J. 229, 229 (1975).

339. John Steven et al., jRapture*: A Capture/Replay Tool for Observation-Based Testing*, 2000 PROC. ACM SIGSOFT INT'L SYMP. ON SOFTWARE TESTING & ANALYSIS 158, 158 (discussing capture/replay capabilities).

340. 45 C.F.R. § 164.312(b) (2007).

Federal Aviation Administration's mandate that certain airplanes be equipped with flight data recorders.[341]

Audit trails and capture/replay would enable experts to determine whether and why EHR system malfunctions occurred and to implement appropriate interventions. Such mechanisms could also assist both defendants and plaintiffs in litigation by facilitating the reconstruction of facts. Furthermore, they could ease the burdens of discovery by allowing for electronic rather than manual searches of records.

Because of the safety-critical nature of EHR systems, there should be a regulatory requirement specifying that the systems include an audit-trail function that details all interactions between systems and their users and all interactions among systems. In order to permit effective system validation and problem diagnosis and resolution, such audit trails ought to include all system input and output that could affect clinical actions or that could reflect the reliability, safety, usability, and security of the system. It must be noted that the accuracy of audit logs may be partially compromised by errors in user input, such as inaccurate recording of body temperature or failure to include physicians' observations concerning patient symptoms. However, in the future, many clinical measurements such as temperature and blood pressure readings could be transmitted directly from instruments to EHRs.

We further recommend that all EHR system vendors be required to support capture/replay capability within a reasonable time after the enactment of the regulations, unless vendors provide compelling technical evidence that doing so would harm the utility or safety of their systems. A reasonable implementation period might be five years, which would give vendors ample time to retrofit capture/replay capability to existing systems, a task that is likely to be more difficult than incorporating this capability into a new design.[342] Vendors, however, should be required to support at least textual audit trails within a much shorter period of time, perhaps one year.

4. Addressing Privacy and Security Concerns

The extraordinarily sensitive nature of personal health information makes it essential for EHR systems to be designed and operated in a way that protects the privacy of patients. In previous work, we have critiqued the HIPAA Security Rule, which governs the security of electronic health information, and have made detailed recommen-

341. 14 C.F.R. § 121.343 (2007).

342. Retrofitting capture/replay capability into an existing system may be difficult for a vendor if the system's external interfaces are excessively complex, if they are no longer well understood due to turnover among the vendor's programming staff, or if the changes negatively affect the efficiency of the system. Also, there is a risk that new defects could be inadvertently introduced into the system, so substantial additional testing is necessary.

dations for enhancing and clarifying its requirements.[343] However, even if these recommendations were adopted in EHR regulations, additional steps would be necessary to address fully the special privacy and security issues raised by interoperability. Interoperability between EHR systems requires a CER.[344] It also requires a common, standardized mechanism by which a provider with a particular EHR system can expeditiously request and receive patient information that is stored on a remote EHR system, even if the two systems were developed by different vendors. This capability in turn requires standardized policies and mechanisms for each of the following: identifying patients and providers; obtaining patients' consent for EHR access; granting appropriate access authorization and privileges to providers; authenticating access requests; and employing cryptographic techniques in order to protect the confidentiality and integrity of EHRs during transmission.[345]

As is true for a common exchange format, standardized security policies and mechanisms are unlikely to be adopted by vendors and providers without a regulatory mandate. In order to facilitate compliance and provide vendors with clear guidance, the regulatory mandate might incorporate, by explicit reference, some established and emerging security standards, such as the Internet Engineering Task Force's Transport Layer Security ("TLS") standard[346] or its Public-Key Infrastructure (X.509) standard.[347]

The prospect of an NHIN has sounded alarms among privacy advocates. Some have suggested that individuals should have the choice of opting out of the NHIN system entirely or of controlling access to their records. For example, the regulations could require that patients

---

343. Hoffman & Podgurski, *supra* note 121, at 359–84 (offering a variety of recommendations for revision of the HIPAA Security Rule to achieve greater data security); Hoffman & Podgurski, *supra* note 115, at 11–14 (developing recommendations and illustrating how they could be implemented); *see also supra* notes 114–28 and accompanying text.

344. *See supra* notes 328–30 and accompanying text (discussing the CER).

345. *See* PRESIDENT'S INFO. TECH. ADVISORY COMM., *supra* note 330, at 30–34 (discussing the need for unambiguous patient identification, encryption, and authentication); Mike Boniface et al., *Accessing Patient Records in Virtual Healthcare Organisations*, ECHALLENGES E-2005, Oct. 20, 2005, *available at* http://eprints.ecs.soton.ac.uk/12224/01/eChallenges2005-final.pdf (discussing patient consent, authentication, authorization, and access control); Dimitris Gritzalis & Costas Lambrinoudakis, *A Security Architecture for Interconnecting Health Information Systems*, 73 INT'L J. MED. INFORMATICS 305, 308 (2004) (discussing encryption); Hiroshi Takeda et al., *An Assessment of PKI and Networked Electronic Patient Record System: Lessons Learned from Real Patient Data Exchange at the Platform of OCHIS (Osaka Community Healthcare Information System)*, 73 INT'L J. MED. INFORMATICS 311–16 (2004) (describing an example of encryption in an EHR system).

346. *See* Transport Layer Security (tls) Charter, http://www.ietf.org/html.charters/tls-charter.html (last visited Dec. 19, 2008).

347. *See* Public-Key Infrastructure (X.509) (pkix) Charter, http://www.ietf.org/html.charters/pkix-charter.html (last visited Dec. 19, 2008).

give specific consent to disclosure of certain types of data, such as mental health histories.[348]

In principle, we oppose this approach. A comprehensive NHIN and full computerization of all health records could not be achieved if individuals were able to opt out fully or partially. A system that included such a choice could be chaotic, in that records would be divided among paper and electronic files and physicians would be unable to access needed information quickly. Moreover, the option could degrade medical care, because physicians, not realizing that patients have carved out certain information, might rely on incomplete medical files. The opt-out alternative could also hinder the transfer of medical data to additional providers when their expertise is needed on an emergency basis, and it could prevent hospital emergency rooms from obtaining information that could save patients' lives. However, we leave open the possibility of allowing patients to sequester sensitive information so long as adequate safeguards are implemented. Such safeguards might include notations in EHRs that information is missing, emergency access to information if patients are unable to provide consent, and the availability of complete medication lists for purposes of ascertaining drug interactions.[349]

Government mandates concerning patient records that limit patient choice are not unprecedented. In *Whalen v. Roe*,[350] the Supreme Court evaluated a constitutional challenge to a New York statute that required that the state be provided with copies of all prescriptions for certain drugs and that specified detailed security measures for the storage of that information. The Court upheld the constitutionality of the statute, finding that it called for a legitimate exercise of the state's police power and that its mandates would not constitute an impermissible invasion of privacy or violation of any Fourteenth Amendment right.[351] Following this precedent, one might reason that government regulations requiring the computerization of all patient records and their inclusion in an NHIN would also be deemed a lawful and constitutional exercise of federal executive power under the Fifth Amendment.[352]

---

348. Terry & Francis, *supra* note 11, at 725–30 (proposing various approaches to incorporating patient choice into EHR systems, including data carve-outs and secure envelopes); *see also* NCVHS, *supra* note 114, at 7 (discussing "[m]ethods of individual control").

349. *See* Letter from Simon P. Cohn, Chairman, Nat'l Comm. Vital Health Statistics, to Michael O. Levitt, U.S. Sec'y of Health & Human Servs. (Feb. 20, 2008), *available at* http://www.ncvhs.hhs.gov/080220lt.pdf (discussing recommendations for the NHIN and describing specific elements that could be left to patient control).

350. 429 U.S. 589 (1977).

351. *Id.* at 602, 606.

352. U.S. CONST. amend. V.

5. Decision Support

Federal regulations should require EHR systems to feature state of the art decision support capabilities.[353] These would include prompts, alerts, treatment suggestions, links to medical literature, and, as technology develops, increasingly sophisticated diagnostic and analytical tools.[354]

To the extent possible, decision support would be based on widely accepted clinical practice guidelines ("CPGs"), which are "[s]ystematically developed statements to assist practitioner and patient decisions about appropriate health care for specific clinical circumstances."[355] For example, a CPG for the treatment of asthma could be incorporated into an EHR system as a checklist that appears when a physician enters information indicating that a particular patient has symptoms consistent with asthma. The feature would alert physicians as to tests that they should conduct, and it would supply treatment suggestions. CPGs have been developed by various organizations, including: professional societies, such as the American Medical Association and other physician specialty boards; governmental entities, such as the AHRQ[356] and various state programs; and health care payers, including health maintenance organizations and health insurers.[357]

At this time, over 2000 CPGs have been published.[358] The CPGs vary in quality,[359] and some may be designed to suit a specific agenda, such as cost-cutting.[360] EHR system vendors cannot be expected to incorporate large numbers of competing and possibly irreconcilable CPGs into their systems, and there is no significant consensus as to which CPGs are the most useful or reliable. Consequently, we recommend that the AHRQ adopt a certification program for CPGs such as the process proposed by Professor Arnold Rosoff.[361] AHRQ would not be the first to endorse guidelines. The FDA recognizes a large

353. *See supra* Part II.B.2 (discussing decision support).

354. *See* CPRS USER GUIDE, *supra* note 39 (detailing features available on the VA's CPRS system).

355. BIOMEDICAL INFORMATICS, *supra* note 1, at 924.

356. *See* AHRQ at a Glance, http://www.ahrq.gov/about/ataglance.htm (last visited Dec. 19, 2008).

357. *See* Michelle M. Mello, *Of Swords and Shields: The Role of Clinical Practice Guidelines in Medical Malpractice Litigation*, 149 U. PA. L. REV. 645, 650 (2001).

358. National Guideline Clearinghouse, http://www.guideline.gov/search/detailed search.aspx (last visited Dec. 19, 2008).

359. Carter L. Williams, Note, *Evidence-Based Medicine in the Law Beyond Clinical Practice Guidelines: What Effect Will EBM Have on the Standard of Care?*, 61 WASH. & LEE L. REV. 479, 491–92 (2004) (analyzing the usefulness of CPGs).

360. Mello, *supra* note 357, at 651.

361. *See* Arnold J. Rosoff, *Evidence-Based Medicine and the Law: The Courts Confront Clinical Practice Guidelines*, 26 J. HEALTH POL., POL'Y & L. 327, 355–65 (2001) (proposing a certification program for CPGs).

number of device-specific consensus standards.[362] It allows applicants seeking device approval to submit abbreviated 510(k) applications[363] when the "FDA has recognized a relevant consensus standard."[364] Furthermore, the FDA will approve devices partly based on conformity to recognized standards.[365] AHRQ could maintain a website listing certified CPGs, much as the FDA maintains a website listing its recognized consensus standards.[366]

EHR system vendors would be expected to incorporate appropriate certified CPGs into their systems, and these could be automatically updated as CPGs change, much as other software updates are automatically downloaded. For example, an EHR system tailored for use in an endocrinologist's office would base decision support on the most up-to-date CPGs for endocrinology, while systems designed for internists or emergency rooms would need to incorporate a broad range of CPGs.

The regulations should require EHR system vendors to use available technology to maximize the efficacy and safety of decision support features. Some researchers have found that decision support does not always change provider behavior.[367] Some physicians may distrust computerized suggestions, may not appreciate a computer telling them how to practice medicine, or may be too busy to consider computerized recommendations carefully,[368] and they may too easily erase prompts by hitting the escape key.[369] The efficacy of decision support can be enhanced through mechanisms such as automatic prompts that do not need to be deliberately initiated, highlighting, periodic remind-

362. The FDA maintains a searchable online database of recognized consensus standards, which currently contains over 700 such standards. Recognized Consensus Standards, http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/Search.CFM (last visited Dec. 19, 2008).

363. *See supra* notes 219–24 and accompanying text (discussing 510(k) applications).

364. U.S. FOOD & DRUG ADMIN. CTR. FOR DEVICES & RADIOLOGICAL HEALTH, THE NEW 510(K) PARADIGM — ALTERNATE APPROACHES TO DEMONSTRATING SUBSTANTIAL EQUIVALENCE IN PREMARKET NOTIFICATION — FINAL GUIDANCE 9 (1998), *at* http://www.fda.gov/cdrh/ode/parad510.pdf.

365. *Id.*

366. *See* Recognized Consensus Standards, *supra* note 362.

367. Amit X. Garg et al., *Effects of Computerized Clinical Decision Support Systems on Practitioner Performance and Patient Outcomes*, 293 JAMA 1223, 1231–32 (2005) (stating that the systems' effects on patient outcomes are not sufficiently studied and are inconsistent when they are examined); Handler et al., *supra* note 60, at 1136 (stating that the benefit of decision support is unclear and often does not seem to affect clinicians' adherence to recommended guidelines).

368. *See* Usha Subramanian et al., *A Controlled Trial of Including Symptom Data in Computer-Based Care Suggestions for Managing Patients with Chronic Heart Failure*, 6 AM. J. MED. 375, 379–80 (2003) (noting that two thirds of suggestions were disregarded).

369. 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 SERV. RES. 477, 492 (2005). When the escape key was disabled, provider adherence to suggestions increased significantly. Dexter et al., *supra* note 62, at 968.

ers, and carefully selected default settings.[370] As a resource for vendors, the regulating agency could include on its website links to literature providing suggestions for maximizing the benefit of decision support mechanisms.

6. Enforcement

The regulations would need to include enforcement provisions in order to ensure compliance. Both EHR system vendors and health care providers must be subject to regulatory enforcement. Vendors would need to ensure that their products conform to regulatory standards and to comply with approval and reporting procedures.[371] Providers would need to adopt approved EHR systems by a specified date and to use them properly in providing clinical care.

EHR system regulation would require the formulation of an enabling statute,[372] and the enabling statute or the implementing regulations would need to include both civil and criminal penalties.[373] The regulatory agency should also be empowered to investigate complaints of non-compliance and to initiate compliance reviews on its own,[374] just as HHS and CMS may investigate covered entities that are suspected of failing to comply with the HIPAA Privacy Rule.[375] If CMS becomes the regulatory agency, the statute and regulations could also provide that noncompliant health care providers will be denied payment for services covered by Medicare, Medicaid, and SCHIP.[376]

---

370. Dexter et al., *supra* note 62, at 968 (noting that displaying a banner on the screen that stated suggestions were available and then requiring physicians to make a deliberate choice to view reminders was ineffective); Garg et al., *supra* note 367, at 1234; McDonald et al., *supra* note 37, at 244–47 (discussing the Regenstrief system's automatic suggestions, which are triggered by various types of data input).

371. *See supra* Part IV.B.

372. Regulatory authority could be included in new legislation or as an amendment to existing legislation, such as HIPAA or the Public Health Service Act. *See* S. 1693, 110th Cong. (2007) (proposing to amend the Public Health Services Act to add HIT provisions).

373. The penalty system could be based on the system that has already been established for HIPAA Privacy Rule violations. *See* 42 U.S.C. §§ 1320d-5 to 1320d-6 (2000); 45 C.F.R. §§ 160.400–.426 (2007) (establishing civil penalties for violations of the HIPAA Privacy Rule).

374. *See* 45 C.F.R. §§ 160.306, .308 (setting out the enforcement model established by the HIPAA Privacy Rule).

375. *Id.*; *see, e.g.*, Jaikumar Vijayan, *HIPAA Audit Riles Health IT: Medical Industry on Edge After Feds Examine Hospital's Security Procedures*, COMPUTERWORLD, June 18, 2007, at 1, 1 (reporting that HHS initiated a HIPAA Security Rule audit of Piedmont Hospital in Atlanta in March 2007).

376. *See* 42 U.S.C. § 1395i-3(h)(2)(B)(i) (authorizing the HHS Secretary to deny payment to skilled nursing facilities that have not met particular requirements); 42 C.F.R. § 488.417 (2007) (providing that noncompliant long term care facilities may be denied Medicare and Medicaid payments for new admissions).

The Joint Commission, formerly the Joint Commission on Accreditation of Healthcare Organizations,[377] could also contribute to enforcement efforts. The Joint Commission is a not-for-profit organization that accredits almost 15,000 U.S. health care organizations and programs according to standards that it develops.[378] Once EHR system adoption becomes mandatory, the Joint Commission could add standards related to EHR systems to its accreditation criteria[379] in order to monitor entities' adoption and effective use of these mechanisms.

Furthermore, the threat of product liability or medical malpractice litigation could deter misconduct by both EHR system vendors and health care providers. Plaintiffs may sue providers if they suspect that they suffered poor outcomes because providers failed to implement or properly use EHR systems, for example, by neglecting to utilize decision-support features that may have averted a medical mistake. Likewise, plaintiffs might name EHR system vendors as defendants if they believe the harm is rooted at least partly in a design flaw, and health care providers might bring in vendors as third party defendants if they believe the vendors to be partially at fault.[380] Audit logs and capture/replay[381] would be helpful to all parties in investigating and proving their claims concerning system failures and provider negligence or lack thereof.

HHS has been accused of providing only anemic enforcement for the HIPAA Privacy Rule and HIPAA Security Rule.[382] Whichever agency is charged with regulating EHR systems will need sufficient funding to engage in robust enforcement activities. However, because plaintiffs can already sue both health care providers and EHR system

---

377. The Joint Commission Launches New Brand Identity, http://www.jointcommission.org/AboutUs/brand.htm (last visited Dec. 19, 2008).

378. Facts about the Joint Commission, http://www.jointcommission.org/AboutUs/Fact_Sheets/joint_commission_facts.htm (last visited Dec. 19, 2008).

379. *See* Standards Frequently Asked Questions, http://www.jointcommission.org/Standards/FAQs/ (last visited Dec. 19, 2008) (elaborating the Joint Commission's current standards).

380. *See* FED. R. CIV. P. 14 (discussing third-party practice). At the same time, EHR system failures might be very difficult to prove because of the products' complexities, and thus the threat of litigation alone might be of somewhat limited value as a deterrent to malfeasance by vendors. *See supra* note 176 and accompanying text.

381. *See supra* Part IV.C.3.

382. *See* Hoffman & Podgurski, *supra* note 121, at 356–57 (discussing HHS enforcement activities); *see also* OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HEALTH & HUMAN SERVS., NATIONWIDE REVIEW OF THE CENTERS FOR MEDICARE & MEDICAID SERVICES HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 OVERSIGHT i–ii (2008), *available at* http://oig.hhs.gov/oas/reports/region4/40705064.pdf (finding that "CMS relied on complaints to identify any noncompliant covered entities that it might investigate. As a result, CMS had no effective mechanism to ensure that covered entities were complying with the HIPAA Security Rule or that [electronic protected health information] was being adequately protected."); Baldas, *supra* note 125, at 4 (stating that, according to some lawyers, "the government is finally putting teeth into a law that has yielded more than 26,000 complaints, but only four convictions").

vendors through the tort system, the statute need not offer a private cause of action to aggrieved individuals. In 2008, the Supreme Court held that federal legislation preempts common law claims that challenge the safety or efficacy of medical devices that have received FDA premarket approval.[383] Because software defects can manifest for the first time long after EHR systems are initially approved,[384] similar preemption of common law claims would be inappropriate for these systems.

D. Improving Health Care Through EHR-based Research

Commentators have noted that the contemporary medical world is characterized by a startling degree of uncertainty.[385] According to some estimates, as few as twenty to twenty-five percent of treatments have been definitively proven effective.[386] EHR systems could contribute significantly to the advancement of medical knowledge by facilitating extensive research initiatives.[387]

The federal regulations could provide for the creation of a vast database consisting of de-identified patient records from hospitals, providers of ambulatory care, long term health care facilities, and all other health care settings. Providers would be required to upload records onto the site on a periodic basis, and the database would be overseen and operated by the designated regulatory agency.

---

383. Riegel v. Medtronic, Inc., 128 S.Ct. 999, 1007–11 (2008). Under *Riegel*, common law claims involving products approved through the 510(k) process are not preempted. *Id.* at 1007.

384. *See supra* notes 193–94 and accompanying text (discussing undetected software defects in the Therac-25 radiation therapy machine that led to six deaths).

385. *See, e.g.*, CROSSING THE QUALITY CHASM, *supra* note 68, at 145 (asserting that it takes 15 to 20 years to translate the discovery of a more efficacious treatment into "routine patient care" and that "adherence of clinical practice to the evidence is highly uneven"); 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, 952 (2005) (observing that a "great deal of uncertainty exists about the 'best' treatment for particular clinical conditions, and about the 'best' way to perform those treatments" and that the "efficacy of most medical treatments has never been proven"); *see also Blue Cross Health Plans Recommend Institute to Study Treatments' Effectiveness*, 6 MED. RESEARCH L. & POL'Y 278, 278 (2007) (reporting that Blue Cross urged Congress "to establish an independent public/private institute to fund research on the comparative effectiveness of various medical treatments, medications, and medical devices").

386. John Carey, *Medical Guesswork: From Heart Surgery to Prostate Cancer, the Health Industry Knows Little About Which Common Treatments Really Work*, BUSINESSWEEK, May 29, 2006, at 72, 72 (asserting that many physicians "say the portion of medicine that has been proven effective is still outrageously low — in the range of 20% to 25%").

387. Kevin M. Fickenscher, *The New Frontier of Data Mining*, HEALTH MGMT. TECH., Oct. 2005, at 26, 26, *available at* http://archive.healthmgttech.com/cgi-bin/arttop.asp?Page=1005/1005new_frontier.htm ("With the advent of the electronic health record, new opportunities for uncovering patterns of care we did not know existed will come to the forefront of medical knowledge.").

Electronic records can be "sanitized" automatically to remove identifying information,[388] but the federal regulations would need to define what constitutes sufficient de-identification.[389] In doing so, they would seek to ensure that data mining techniques cannot be used to infer patient identities from a combination of sanitized records and other available data.[390] Although patients should not be allowed to opt out of inclusion in EHR systems and the NHIN,[391] they should be provided a choice concerning inclusion in the research database. Patients would be asked to sign a consent form at the time of their initial visit to a provider or admission to a health care facility indicating their agreement or refusal to have their de-identified EHRs entered into the national research database.[392] With sufficient reassurance that records will in fact be de-identified and that their confidentiality will be protected, many patients may consent to inclusion of their records in the database.

Research using this information could be conducted with few regulatory burdens. De-identified records do not require IRB review and are not subject to coverage by the HIPAA Privacy Rule.[393] The databank would be accessible to qualified researchers who register with the regulatory agency and meet its criteria for approval. Agency review committees could scrutinize applications, and the agency could require applicants to prove their identities and affiliations and to provide a limited description of the planned research projects, along with

388. Matt Bishop et al., *How to Sanitize Data*, 2004 PROC. 13TH IEEE INT'L WORKSHOPS ON ENABLING TECHS.: INFRASTRUCTURE FOR COLLABORATIVE ENTERS. 217, 217, *available at* http://nob.cs.ucdavis.edu/~bishop/papers/2004-wetice/basicsani.pdf (explaining that when sanitization is implemented, "the raw data is presented for others to analyze, but the data is transformed so that sensitive items are suppressed," as is the case when researchers are given patient records from which identifying information, such as name, address, and phone number are expunged).

389. 45 C.F.R. § 164.514(a)–(b) (2007) (stating the HIPAA Privacy Rule's specifications of what constitutes de-identified data).

390. Vassilios S. Verykios et al., *State-of-the-Art in Privacy Preserving Data Mining*, 33 SIGMOD REC. 50, 50–57 (2004), *available at* http://www.sigmod.org/record/issues/0403/B1.bertion-sigmod-record2.pdf ("[S]ensitive knowledge which can be mined from a database by using data mining algorithms, should also be excluded, because such a knowledge can equally well compromise data privacy.").

391. *See supra* text accompanying note 349.

392. Patients should also be able to withdraw consent to having new information submitted to the databank. However, it might not be at all feasible to expunge existing medical records concerning a particular patient, because they may be in use by various researchers.

393. The federal regulations that require IRB review cover only research on human subjects and define "human subject" as "a living individual about whom an investigator . . . obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information." 45 C.F.R. § 46.102; *see also Id.* § 46.101(b)(4) (exempting research "involving the collection or study of existing data, documents, [or] records . . . if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects"). Likewise, the HIPAA Privacy Rule covers only "individually identifiable health information." *See Id.* § 160.103 (defining "protected health information").

other relevant information. Access to the databank would be granted for a period limited to the duration of the study.

The scientific community is already familiar with the Coriell Institute for Medical Research, which maintains one of the world's largest repositories of human cells.[394] The institute has distributed over 160,000 cell lines and over 50,000 DNA samples a year to researchers in sixty-two countries.[395] The proposed databank would constitute a similar resource, containing health records rather than biological samples.

The databank would enable researchers to conduct comprehensive, non-experimental studies based on the actual clinical experience of patients and care givers.[396] The importance of such research capabilities has already been recognized by the federal government. In 2007, Congress authorized the FDA to oversee the creation of a national data network, the Sentinel System. This project aims ultimately to make the data of 100 million Americans available for purposes of post-marketing drug surveillance and safety analysis. The data will be drawn from records from Medicare, the military, private insurance claims, pharmaceutical purchases, and elsewhere.[397]

The research databank proposed in this Article would go much further than this initiative. It could potentially include the records of all Americans, be accessible to government and to private researchers, and be used to study all treatments rather than focusing only on those involving pharmaceutical products. Once created, this databank could replace all smaller-scale data collections.

While research derived from the proposed national databank would not be a substitute for clinical trials, it would constitute an invaluable supplement to them. Researchers would be able to verify the success or failure of treatment protocols as they are applied to different patient populations, based on review of millions of patient files covering many years.

V. CONCLUSION

EHR systems offer great promise for significantly improving health care in the U.S. and around the world. The technology could address many of the health care system's shortcomings and have far-

394. *See* Coriell Institute for Medical Research — About Coriell, http://www.coriell.org/index.php/content/view/110/234/ (last visited Dec. 19, 2008).

395. *Id.*

396. *See supra* notes 84–100 and accompanying text (comparing experimental and non-experimental studies).

397. *See* 21 U.S.C.A. § 355(k) (West 1999 & Supp. 2008); Barbara J. Evans, *Congress' New Infrastructural Model of Medical Privacy*, 84 NOTRE DAME L. REV. (forthcoming Feb. 2009) (manuscript at 2–4), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1186462.

reaching positive impacts on patient welfare. For example, HIT could do all of the following: decrease medical errors; enhance preventive care; facilitate communication between doctors and patients and among medical team members; reduce health disparities; and advance biomedical research capabilities.

The complexity of EHR systems, however, generates many risks of software and hardware failures and adverse patient outcomes. Consequently, they require rigorous regulation. Some risks can stem from system defects and others from usability problems. Advanced EHR systems that will be developed in the future could improve health outcomes to an even greater extent, but they may also pose more serious risks because of increased complexity.

Although EHR system regulation is needed, it is a challenging and sensitive undertaking. A tension exists between the goals of regulating EHR systems comprehensively and facilitating their widespread and imminent adoption. The more extensive and burdensome the regulations, the more providers will resist purchasing EHR systems. We have attempted to craft a balanced approach that provides incentives for EHR system development and adoption while safeguarding patient welfare and deterring misconduct on the part of the software and health care industries. As laws and regulations are promulgated in this area, policy makers will need to continue to consider carefully the competing goals and to balance oversight with promotion of HIT.

Innumerable details and requirements could be included in the federal regulations. We have not offered comprehensive suggestions or specific regulatory language. Rather, we outlined a regulatory framework and focused on what we believe to be some of the essential issues in the realm of EHR system oversight. The task of EHR system regulation, however, must commence at the earliest opportunity. It is only with appropriate statutory and regulatory interventions that the full benefits of this potentially transformative medical technology can be realized.