2009

E-Health Hazards: Provider Liability and Electronic Health Record Systems

Sharona Hoffman

Andy Podgurski
Case Western University, andy@eecs.case.edu

E-HEALTH HAZARDS: PROVIDER LIABILITY AND ELECTRONIC HEALTH RECORD SYSTEMS

Sharona Hoffman[†] *& Andy Podgurski* [††]

ABSTRACT

In the foreseeable future, electronic health record (EHR) systems are likely to become a fixture in medical settings. The potential benefits of computerization could be substantial, but EHR systems also give rise to new liability risks for health care providers that have received little attention in the legal literature. This Article features a first of its kind, comprehensive analysis of the liability risks associated with use of this complex and important technology. In addition, it develops recommendations to address these liability concerns. Appropriate measures include federal regulations designed to ensure the quality and safety of EHR systems along with agency guidance and well crafted clinical practice guidelines for EHR system users. In formulating its recommendations, the Article proposes a novel, uniform process for developing authoritative clinical practice guidelines and explores how EHR technology itself can enable experts to gather evidence of best practices. The authors argue that without thoughtful interventions and sound guidance from government and medical organizations, this promising technology may encumber rather than support clinicians and may hinder rather than promote health outcome improvements.

TABLE OF CONTENTS

---

† Professor of Law and Bioethics, Co-Director of Law-Medicine Center, 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 of Electrical Engineering and Computer Science, Case Western Reserve University. B.S., M.S., Ph.D., University of Massachusetts. The authors wish to thank Jessica Berg, Henry Bloom, Shawneequa Callier, David Hyman, Richard Krueck, Maxwell J. Mehlman, Cassandra Robertson, and Robert Strassfeld for valuable comments on drafts of this paper. We are also grateful for the very skillful research assistance of Michael Hill.

I. INTRODUCTION

The American Recovery and Reinvestment Act of 2009 (ARRA),[1] better known as President Obama's stimulus legislation, was enacted to rescue an

1. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

ailing economy in early 2009.[2] One of its many goals was "to increase economic efficiency by spurring technological advances in science and health."[3] To that end, ARRA dedicated nineteen billion dollars to the promotion of health information technology.[4]

The ARRA's goal is to computerize all Americans' health records by 2014.[5] Currently, only a small minority of health care practices use electronic health record (EHR) systems, including perhaps seventeen percent of doctors and ten percent of hospitals.[6] In order to comply with this mandate and avoid penalties for non-compliance,[7] health care providers will need to increase their rate of EHR system adoption dramatically.

Comprehensive EHR systems will have a pervasive influence on medical care and serve multiple functions beyond storing medical files. They electronically transmit diagnostic test images and results, laboratory reports, and radiologic images and reports to physicians so that these can be quickly reviewed and shared with patients.[8] The systems feature computerized provider-order entry (CPOE), which allows providers to send electronic orders, such as those for laboratory tests and medications, to appropriate parties.[9] They also feature decision support tools, among which are clinical guidelines, clinical reminders, drug-allergy and drug interaction alerts, and drug-dose support.[10] EHR systems may also provide a secure messaging feature to help physicians communicate with patients confidentially.[11] Ideally, EHR systems should be interoperable and thus be able to automatically

2. *Id.* at § 3 (stating that the purpose of the Act is "to preserve and create jobs and promote economic recovery" and "to assist those most impacted by the recession").

3. *Id.* § 3(a)(3).

4. David Blumenthal, *Stimulating the Adoption of Health Information Technology*, 360 NEW ENG. J. MED. 1477 (2009).

5. American Recovery and Reinvestment Act § 3001(c)(3)(A)(ii).

6. *Id.* (noting that these figures represent practices using basic systems, not necessarily sophisticated or comprehensive systems); Catherine M. DesRoches et al., *Electronic Health Records in Ambulatory Care: A National Survey of Physicians*, 359 NEW ENG. J. MED. 50, 54 (2008); Ashish K. Jha et al., *Use of Electronic Health Records in U.S. Hospitals*, 360 NEW ENG. J. MED. 1628, 1631 (2009).

7. Blumenthal, *supra* note 4, at 1477–78 (noting that "[p]hysicians who are not using EHRs systems meaningfully will lose 1% of their Medicare fees in 2015, then 2% in 2016, and 3% in 2017").

8. Jha et al., *supra* note 6, at 1632.

9. *Id.*

10. *Id.*

11. Catherine Chen et al., *The Kaiser Permanente Electronic Health Record: Transforming And Streamlining Modalities of Care*, 28 HEALTH AFF. 323, 325 (2009) (describing the secure messaging system implemented by Kaiser Permanente Hawaii in September 2005).

incorporate records and process information from EHR systems developed by different vendors.[12]

The potential benefits of computerization are considerable.[13] In short, EHR systems can facilitate access to patients' medical records, improve the quality of care and the accuracy of treatment decisions, achieve cost savings, and promote clinical research.[14] Some health care providers with EHR systems already report better outcomes, fewer complications, lower costs, and fewer malpractice claim payments.[15] Without discounting any of these potential benefits, this Article focuses on the risks of EHR systems and on liability concerns associated with their use. It argues that despite the promise of this technology, the implementation of EHR systems must proceed with both caution and appropriate government oversight.

In recent years, more than a few startling EHR-related stories have surfaced. For example, software glitches in the U.S. Department of Veterans Health Administration's EHR system exposed veterans to excessive,

---

12. BIOMEDICAL INFORMATICS: COMPUTER APPLICATIONS IN HEALTH CARE AND BIOMEDICINE 952 (Edward H. Shortliffe & James J. Cimino eds., 2006) [hereinafter BIOMEDICAL INFORMATICS] (explaining that interoperable systems can communicate with each other, exchange data, and operate seamlessly and in a coordinated fashion across organizations).

13. We have discussed them extensively in prior work. *See* Sharona Hoffman & Andy Podgurski, *Finding A Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 HARV. J.L. & TECH. 103, 112–19 (2008) (discussing the benefits of EHR systems).

14. *Id.*; *see also* Richard J. Baron et al., *Electronic Health Records: Just Around the Corner? Or Over the Cliff?* 143 ANNALS INTERNAL MED. 222, 225–26 (2005) (discussing the benefits of an EHR system in a small practice); Stephen T. Parente & Jeffrey S. McCullough, *Health Information Technology And Patient Safety: Evidence From Panel Data*, 28 HEALTH AFF. 357, 357–58 (2009) (utilizing four years of inpatient data from Medicare patients and finding that EHRs have "a small, positive effect on patient safety"); Julie Weed, *If All Doctors Had More Time to Listen*, N.Y. TIMES, June 7, 2009, at BU1 (praising EHR systems and arguing that they save physicians time and money). *But see* Yong Y. Han et al., *Unexpected Increased Mortality After Implementation of a Commercially Sold Computerized Physician Order Entry System*, 116 PEDIATRICS 1506, 1510–12 (2005) (noting that the mortality rate among children increased from 2.80% to 6.57% after computerized physician order entry implementation and asserting that further evaluation of this evolving technology is needed).

15. Ruben Amarasingham et al., *Clinical Information Technologies and Inpatient Outcomes*, 169 ARCH. INTERN. MED 108, 111–12 (2009) (reporting on a survey that involved 167,233 patients at 41 urban Texas hospitals); Anunta Virapongse et al., *Electronic Health Records and Malpractice Claims in Office Practice*, 168 ARCH. INTERN. MED. 2362, 2365 (2008) (presenting a survey of 1,345 Massachusetts physicians and stating that although the study's results were inconclusive, they suggest that "physicians with EHRs appear less likely to have paid malpractice claims"). *But see* Steve Lohr, *Little Benefit Seen, So Far, in Electronic Patient Records*, N.Y. TIMES, Nov. 16, 2009, at B3 (reporting on research that revealed that EHR systems have "not yet had a real impact on the quality or cost of health care").

potentially life-threatening dosages of the blood-thinner heparin.[16] In a different incident, a hospital pharmacy's computer program generated erroneous medication order lists, leading to the delivery of the wrong drugs to patients in many wards.[17] A May 2009 article featured the alarming title " 'Nearly Killed' by E-Records Data Model" and described the distressing experience of a patient in an intensive care unit with an EHR system that did not allow doctors and nurses to access critical medical information or obtain medication from the pharmacy in a timely fashion.[18] The liability risks of EHR systems, however, have received little attention in the legal literature.

Along with the potential to enhance health outcomes, this new technology may bring novel responsibilities, burdens, and complexities for medical practices. Historically, medical innovations, such as anesthetics and x-rays, have generated increased tort litigation as patients quickly came to expect better care while physicians struggled to perfect their use of challenging technologies.[19] The same phenomenon may well occur with EHR systems. This Article details specific liability risks associated with EHR systems and explores strategies to alleviate liability concerns.[20] For the sake of simplicity, we use the terms EHR and EHR systems to designate electronic health records and the systems in which they operate. We mean the term EHR to be synonymous with what others call the electronic medical record (EMR).[21]

---

16. Hope Yen, BlueCross BlueShield Association, Veterans Exposed to Incorrect Drug Doses, (Jan. 13, 2009), http://www.bcbs.com/news/national/veterans-exposed-to-incorrect-drug-doses.html.

17. Richard I. Cook & Michael F. O'Connor, *Thinking About Accidents and Systems*, *in* IMPROVING MEDICATION SAFETY 80, 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. Tony Collins, *"Nearly Killed" by E-Records Data Model*, COMPUTERWEEKLY.COM, (May 21, 2009), http://www.computerweekly.com/Articles/2009/05/21/236128/nearly-killed-by-e-records-data-model.htm.

19. James C. Mohr, *American Medical Malpractice Litigation in Historical Perspective*, 283 J. AM. MED. ASS'N 1731, 1733–34 (2000); Mark F. Grady, *Why Are People Negligent? Technology, Nondurable Precautions, and the Medical Malpractice Explosion*, 82 NW. U. L. REV. 293, 297–301, 314–15 (1988) (explaining that many "believe that new technology adds to the number of negligence claims" and analyzing the reasons for this phenomenon).

20. *See infra* Part IV.

21. There is confusion in the literature about the terms EHR and EMR. For example, the HITECH Act defines an EHR as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff." American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) (to be codified at 42 U.S.C. § 17921(5)). However, one commentator notes that the HITECH Act's definition of EHR is "confusingly . . . one that is generally associated with an EMR." Nicolas P. Terry, *Personal Health Records: Directing More Costs and*

With their wealth of capabilities, EHR systems are likely to raise the public's expectations concerning clinicians' performance and to affect the standard of care to which clinicians are held for medical malpractice purposes.[22] The systems make unprecedented volumes of information available to physicians.[23] With computers connecting them to a local, regional, and perhaps even national health information network,[24] doctors could have access to every detail of the patient's medical history from birth until the present time and be expected to consider all relevant information in their treatment decisions. EHR systems also provide doctors with sophisticated decision support tools,[25] which will raise the public's expectations concerning the quality of medical treatments. More common use of e-mail and secure messaging for patient-doctor communication and improved access to clinical data through personal health records[26] may further increase patient demands and expectations.

Physicians who have more complete records and better decision support and communication tools, but who do not have the time or skill to assimilate the unprecedented amount of available data and to optimize their use of technology, may face medical malpractice claims that would have never emerged in the past.[27] Clinicians who mishandle EHR systems and thereby cause injury to patients could also in rare cases face disciplinary action initiated by state licensing boards and even criminal prosecution.[28] Health care organizations such as hospitals may likewise face reaccreditation challenges and lawsuits based on vicarious liability and other negligence theories.[29]

Risks to Consumers?, 1 DREXEL L. REV. 216, 257 (2009).

22. *See infra* notes 69–79 and accompanying text for a discussion of medical malpractice and the standard of care.

23. Jha et al., *supra* note 6, at 1633 (discussing the various capabilities of comprehensive EHR systems).

24. American Recovery and Reinvestment Act § 3002(b)(1) (articulating the goal of establishing a "nationwide health information technology infrastructure that permits the electronic exchange and use of health information").

25. Jonathan A. Handler et al., *Computerized Physician Order Entry and Online Decision Support*, 11 ACAD. EMERGENCY MED. 1135, 1135–36 (2004).

26. *See* 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, 121 (2006) (explaining that personal health records provide a "repository for patient data," provide capabilities that "assist patients in managing chronic conditions," and generally allow individuals to be more active in their own health care).

27. *See infra* Section III.A.2.

28. *See infra* Section III.C.

29. *See infra* Sections III.A.1 & III.C.

In addition, computerization and electronic distribution of private health information could lead to privacy breach claims. Electronic data is vulnerable to improper disclosure through hacking, laptop theft, inadvertent disclosure, or deliberate leaks.[30] Once electronic information is accessed by unauthorized personnel, it can be rapidly distributed to a worldwide audience through the Internet, potentially causing humiliation, ruining careers, or causing other serious harms.[31]

This Article provides a first of its kind, comprehensive analysis of the liability risks associated with EHR systems, which may soon become a fixture in all medical settings. It considers the mandates of the Health Information Technology for Economic and Clinical Health Act (HITECH Act),[32] the portion of the ARRA that focuses on health information technology. Part II describes EHR systems and how they function in the contemporary medical practice setting. Part III analyzes new liability risks associated with EHR systems.

Part IV then formulates recommendations to address liability concerns. In particular, we argue that EHR systems, which are currently an unregulated technology,[33] must be regulated by the federal government in order to achieve quality control.[34] In addition, agency guidance and clinical practice guidelines should assist providers in optimizing EHR system use.[35] This Article explores how the standard of care should be established with respect to an emerging technology with a very limited use history. It proposes a new, uniform process for the development of clinical practice guidelines that is coordinated by a central professional organization and is based on field evaluation. It also suggests that EHR systems' own audit trails[36] and electronic search capabilities could contribute much to the formulation of sound guidelines concerning operating standards. Regulations, agency guidance, and widely accepted, authoritative clinical practice guidelines would all constitute admissible evidence of the standard of care and provide some degree of predictability for litigation purposes at the same time that they help clinicians maximize the benefits and minimize the risks of EHR system use.[37]

---

30. Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 332–34 (2007).

31. *Id.* at 332.

32. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13001, 123 Stat. 115, 226 (2009).

33. *See* Hoffman & Podgurski, *supra* note 13, at 126.

34. *See infra* Section IV.A.1.

35. *See infra* Section III.A.2 & IV.B.2.

36. *See infra* notes 336–39 and accompanying text.

37. *See infra* Section IV.B.

II. EHR SYSTEM ATTRIBUTES

An EHR can be defined as a "repository of electronically maintained information about an individual's lifetime health status and health care."[38] An EHR system is the "addition to an electronic health record of information management tools."[39] Comprehensive EHR systems provide a broad range of functions.[40] They assist providers in managing health information and data by displaying laboratory test results, allergies, lists of other medications the patient is taking, medical and nursing diagnoses, patient demographics, and providers' notes.[41] EHR systems also transmit results from laboratory tests, radiology procedures, and other diagnostic examinations electronically so that providers can quickly and efficiently access needed information.[42] Many systems allow clinicians to submit computerized medication orders and other care instructions, which can reduce or eliminate lost orders, duplicate orders, mistakes caused by illegible handwriting, and delays in filling orders.[43]

Of particular importance and complexity are EHR systems' decision support features. Automatic reminders and prompts can improve preventive care, diagnosis, treatment, and disease management.[44] For example, an EHR system can remind providers that a patient needs a vaccination or mammogram or that the patient is allergic to a medication that the doctor wishes to prescribe. More sophisticated systems might even analyze entered data and suggest appropriate diagnostic tests, diagnoses, or treatment plans.[45]

EHR systems can optimize connectivity and communication.[46] They can facilitate online communication among medical team members, between clinicians and other providers such as laboratories or pharmacies, and between caregivers and their patients. Communication can be achieved through e-mail, web messaging, integrated health records within and across treatment settings, telemedicine,[47] and home telemonitoring.[48] Once in place,

---

38. BIOMEDICAL INFORMATICS, *supra* note 12 at 937.

39. *Id.*

40. INSTITUTE OF MEDICINE, KEY CAPABILITIES OF AN ELECTRONIC HEALTH RECORD SYSTEM 7–9 (2003) [hereinafter KEY CAPABILITIES].

41. *Id.* at 7.

42. *Id.* at 7–8.

43. *Id.* at 8.

44. *Id.* at 8–9.

45. Handler et al., *supra* note 25, at 1135–36 (discussing systems that assist in diagnosis and therapeutic decisions).

46. KEY CAPABILITIES, *supra* note 40, at 9.

47. Telemedicine is "the delivery of health care at a distance, increasingly but not exclusively by means of the Internet." BIOMEDICAL INFORMATICS, *supra* note 12, at 991.

48. 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."

an EHR system may become the primary means of communication among clinicians.

As stated in the Health Information Technology for Economic and Clinical Health (HITECH) Act, the federal government's goal is to achieve interoperability by building a "nationwide health information technology infrastructure that permits the electronic exchange and use of health information."[49] "Interoperability" means the ability of two or more systems to exchange data and to operate in a coordinated fashion.[50] With interoperability, authorized personnel would be able to access patient records regardless of where they are stored and by whom the patient was previously treated, including records compiled by providers in distant locations and other health care networks.[51] This capability would allow doctors to discover information about a new patient's medical history, drug lists, allergies, and other critical matters for which they currently must depend upon the patient's memory. Furthermore, emergency room personnel treating unconscious or uncommunicative patients would no longer need to operate in complete ignorance of crucial medical facts.[52] However, interoperability will dramatically expand the amount of information clinicians must read and consider in treating their patients. It will also increase the risk of inappropriate disclosure because individuals across the country may be able to access a patient's records.

One component of some EHR systems that is particularly appealing to patients is the personal health record (PHR). A PHR has been defined as "an electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment."[53]

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).

49. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3002(b)(1), 123 Stat. 115, 234 (2009) (to be codified at 42 U.S.C. § 300jj-12(b)(1)).

50. BIOMEDICAL INFORMATICS, *supra* note 12, at 952.

51. Hoffman & Podgurski, *supra* note 13, at 112–13.

52. They could also have immediate access to important documents such as a living will or durable power of attorney for health care.

53. Tang et al., *supra* note 26, at 122 (citing MARKLE FOUNDATION, CONNECTING FOR HEALTH: THE PERSONAL HEALTH WORKING GROUP FINAL REPORT (2003), http://www.connectingforhealth.org/resources/final_phwg_report1.pdf; *see also* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13400(11), 123 Stat. 115, 259 (2009) (to be codified at 42 U.S.C. § 17921(11)), (defining a PHR as an "electronic record of . . . health information . . . on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual").

PHRs are found in various forms. Some are web pages that allow patients to enter their own health information; others are physician-provided patient portals that allow patients to access part or all of their EHRs; and still others are constructed by employers or insurers and enable patients to review their claims data.[54] For example, an independent vendor, Epic Systems, has developed a PHR called MyChart that allows patients to read their EHRs, including lab test results, and to communicate electronically with physicians through secure messaging, but it does not provide access to progress notes.[55] MyChart, which is integrated with an EHR system, is hosted by medical practices, and is used by 2.4 million U.S. patients, according to recent estimates.[56]

A second PHR model is PatientSite, a hospital-based system built by Beth Israel Deaconess Medical Center. PatientSite allows patients to access their lists of problems, medications, allergies, visit schedules, and laboratory and other diagnostic test results.[57] In addition, patients can add information to their PHRs, such as readings from home-administered tests, records of over-the-counter drugs that they take, and personal notes.[58] Furthermore, the system provides for secure messaging, automated appointment scheduling, prescription renewals, and specialist referrals.[59]

Still other PHRs are independent, personally-controlled products.[60] The patients decide who can review, write, or change these health records.[61] Such PHRs could exchange data with EHR systems or function as stand-alone records that are supplied on smart cards, CDs, or USB drives.[62]

Only a minority of medical practices currently use EHR systems to a significant extent. According to a recent survey, only 2.9 percent of U.S. hospitals have comprehensive EHR systems "across all major clinical units."[63] An additional 7.9 percent of hospitals have basic systems that include electronic clinicians' notes in at least one clinical unit, and 11.3 percent have basic systems that do not include electronic clinicians' notes.[64]

---

54. John D. Halamka, *Early Experiences with Personal Health Records*, 15 J. AM. MED. INFORMATICS ASS'N 1, 1 (Jan./Feb. 2008).

55. *Id.* at 1–2.

56. *Id.* at 1.

57. *Id.* at 2.

58. *Id.*

59. *Id.*

60. *Id.* at 2–3.

61. *Id.* (describing Indivo, a personally controlled health record).

62. *Id.* at 3; Tang et al., *supra* note 26, at 122.

63. This figure includes Veterans Health Administration hospitals. Jha, *supra* note 6, at 1631.

64. *Id.*

A basic system includes electronic notes concerning patient demographics, medical problem lists, medication lists, discharge summaries, laboratory reports, radiologic reports, and diagnostic test results, but excludes clinicians' notes.[65] Seventy-five percent of hospitals have adopted electronic laboratory and radiologic test result reporting, and seventeen percent have CPOE.[66] An earlier survey focusing on ambulatory care concluded that only four percent of physicians had comprehensive EHR systems, while thirteen percent had basic systems.[67]

New technologies have the potential to improve health outcomes and patient satisfaction dramatically. However, they may also create significant challenges for clinicians by generating increased workloads, unrealistic patient expectations, privacy breaches, and the likelihood of computer-related mishaps that endanger patient welfare. Consequently, health care providers may be faced with new litigation vulnerabilities that did not emerge during the era of paper medical records.[68]

III. LIABILITY CONCERNS

This section provides a comprehensive overview of the liability risks faced by EHR system users. Contemporary EHR system technology has significant limitations, and if these cause harm, aggrieved individuals and enforcement entities have many legal resources. Plaintiffs whose alleged injuries are associated with EHR systems could sue health care providers for medical malpractice. Those who believe that their records have been improperly disclosed to third parties could assert privacy violation claims. In rare circumstances, providers accused of negligent EHR system use could face disciplinary proceedings (initiated by professional organizations), government enforcement actions, or criminal prosecutions. Each of these potential claims and penalties will be addressed below.

A. MEDICAL MALPRACTICE CLAIMS

Patients who feel that their care givers were negligent in treating them may assert medical malpractice claims. To prevail, the plaintiff must establish

65. *Id.* at 1633.

66. *Id.* at 1631.

67. DesRoches et al., *supra* note 6, at 50, 54. The difference between basic and fully functional EHR systems is discussed *id.* at 52.

68. Shana Campbell Jones et al., *The Interoperable Electronic Health Record: Preserving Its Promise by Recognizing and Limiting Physician Liability*, 63 FOOD & DRUG L.J. 75, 81 (2008) (noting that physicians may eschew EHR system adoption if they are alarmed by the prospect of "expanded professional liability exposure").

the four elements of negligence:[69] (1) a duty of care owed by the defendant to the plaintiff, (2) breach of that duty through conduct that fails to meet the applicable standard of care, (3) harm or injury, and (4) a causal link between the injury and the breach of duty.[70] The standard of care in each case is determined based on an assessment of whether the defendant "proceed[ed] with such reasonable caution as a prudent man would have exercised under such circumstances."[71] Thus, in medical malpractice cases, plaintiffs must prove that "the professional failed to conform to the generally recognized and accepted practices in his profession."[72]

As evidenced by the phrase "accepted practices," medical malpractice jurisprudence establishes that the legal standard of care is determined by professional custom.[73] Deviation from custom can constitute conclusive proof of negligence.[74] Physicians are not required to provide *optimal* care in order to avoid liability, but rather they are required to provide the level of care that could ordinarily be expected.[75]

One further question is whether professional custom should be judged based on practices in a narrow geographic location, such as the defendant's own community, or whether the area of focus should be broader, perhaps even national.[76] Although early decisions adhered to a "strict locality" rule,

69. Eleanor D. Kinney, *Administrative Law Approaches to Medical Malpractice Reform*, 49 ST. LOUIS U. L.J. 45, 49 (2004).

70. PROSSER & KEETON ON THE LAW OF TORTS (W. Page Keeton et al. eds., 5th ed. 1984).

71. Vaughan v. Menlove, (1837) 132 Eng. Rep. 490, 492 (C.P.) (affirming a jury verdict for the plaintiff who was injured when a fire that began in the defendant's haystack burnt down his house).

72. Doe v. Am. Red Cross Blood Servs., 377 S.E.2d 323, 326 (S.C. 1989).

73. RESTATEMENT (THIRD) OF TORTS § 13 cmt. b (Proposed Draft No. 1, 2005) ("In professional-malpractice cases, the malpractice standard is to a significant extent defined in terms of professional standards and customs."); Michelle M. Mello, *Of Swords and Shields: The Role of Clinical Practice Guidelines in Medical Malpractice Litigation*, 149 U. PA. L. REV. 645, 654–58 (2001) (discussing the role of professional custom in standard of care analysis in medical malpractice cases).

74. RESTATEMENT (THIRD) OF TORTS, *supra* note 73, § 13 cmt. b; Mello, *supra* note 73, at 658. *Cf.* Hood v. Phillips, 554 S.W.2d 160, 165 (Tex. 1977) ("A physician who undertakes a mode or form of treatment which a reasonable and prudent member of the medical profession would undertake . . . shall not be subject to liability."); Jeffrey J. Rachlinski, *A Positive Psychological Theory of Judging in Hindsight*, 65 U. CHI. L. REV. 571, 612 (1998) ("Doctors who have followed customary medical procedure are not to be considered negligent."). *But see* Tim Cramm et al., *Ascertaining Customary Care in Malpractice Cases: Asking Those Who Know*, 37 WAKE FOREST L. REV. 699, 707–10 (2002) (discussing an "incipient trend towards modifying custom as conclusive" and moving closer to the traditional reasonable standard for negligence cases).

75. Cramm et al., *supra* note 74, at 702.

76. *Id.* at 705–07; BARRY R. FURROW ET AL., HEALTH LAW CASES, MATERIALS AND

most states currently follow a "similar locality" or national standard.[77] Interoperable EHR systems would make a national professional custom rule more sensible because records will be nationally accessible and transmittable and because decision support could provide clinicians across the country with state of the art information and support.[78] Interoperability would not preclude defendants from presenting evidence that they had more limited resources at their particular institutions since establishing the standard of care requires consideration of the specific circumstances at issue.[79]

1. Liability of Health Care Entities: Corporate Negligence and Vicarious Liability

Medical malpractice claims can be asserted against health care entities such as hospitals and clinics under the theories of corporate negligence and vicarious liability.[80] In corporate negligence cases, health care organizations can be held liable for failing to safeguard their patients' safety and welfare.[81] Hospitals have the following four duties:

> (1) a duty to use reasonable care in the maintenance of safe and adequate facilities and equipment; (2) a duty to select and retain only competent physicians; (3) a duty to oversee all persons who practice medicine within its walls as to patient care; and (4) a duty to formulate, adopt and enforce adequate rules and policies to ensure quality care for the patients.[82]

In establishing a prima facie case of corporate negligence, plaintiffs must show (1) that the hospital deviated from the standard of care; (2) that the hospital has actual or constructive knowledge of the flaws or procedures that

---

PROBLEMS 338–39 (6th ed. 2008).

77. Cramm et al., *supra* note 74, at 705–07; FURROW ET. AL., *supra* note 76, at 338 (explaining the concern that a strict locality rule would make it very difficult for plaintiffs to find expert witnesses because physicians would be reluctant to testify against colleagues in their own communities).

78. Cramm et al., *supra* note 74, at 706 (noting that the globalization of information supports moving away from a locality rule).

79. *See supra* note 71 and accompanying text; FURROW ET AL., *supra* note 76, at 338 (citing RESTATEMENT (SECOND) OF TORTS § 299A cmt. d (1965)). ("A country doctor cannot be expected to have the equipment, facilities, experience, knowledge or opportunity to obtain it, afforded him by a large city.").

80. Darling v. Charleston Cmty. Mem'l Hosp., 211 N.E.2d 253 (Ill. 1965) (recognizing a cause of action for corporate negligence); Alexander v. Mount Sinai Hosp. Medical Center, 484 F.3d 889, 903 (7th Cir. 2007) (explaining how plaintiff could sustain a medical malpractice claim against the hospital based on vicarious liability).

81. Thompson v. Nason Hosp., 591 A.2d 703, 707 (Pa. 1991).

82. *Id.*

caused the injury; and (3) that a causal link exists between the conduct and the harm.[83]

Organizations can also be held liable for the actions of their employees through the vicarious liability theories of respondeat superior and ostensible agency. The doctrine of "respondeat superior," which literally means "let the superior answer," establishes that employers are responsible for the acts of their employees in the course of their employment.[84] Thus, hospitals may be held liable for inappropriate EHR system uses by nurses, residents, interns, or other health professionals. However, in many instances, hospitals are shielded from liability for physicians' acts because physicians are considered independent contractors rather than employees.[85] Nevertheless, courts have found that a hospital's imposition of workplace rules and regulations upon staff physicians is enough to undercut the doctors' independent contractor status and expose the hospital to liability.[86] Therefore, hospitals that establish EHR-use protocols and policies may be responsible for clinicians' negligent operation of these systems.

An alternative theory of liability is ostensible agency. A hospital can be liable for an independent contractor's wrongdoing if the individual is deemed to be the hospital's "ostensible agent."[87] A court can find ostensible agency if (1) the patient looks to the entity rather than the specific physician for care, and (2) the hospital "holds out" the doctor as its employee.[88] The ostensible agency theory is particularly applicable to emergency room care, because patients generally seek medical treatment from emergency departments rather than from individual attending physicians.[89]

---

83. Rauch v. Mike-Mayer, 783 A.2d 815, 827 (Pa. Super. Ct. 2001).

84. BLACK'S LAW DICTIONARY 1338 (8th ed. 2004) (defining the term to mean that employers are responsible for the acts of their employees in the course of their employment).

85. *See, e.g.*, Kashishian v. Port, 481 N.W.2d 277, 280 (Wis. 1992) (holding that even though a physician was a member of the hospital's staff and was required to comply with hospital policies, no master-servant relationship existed); Albain v. Flower Hosp., 553 N.E.2d 1038, 1044 (Ohio 1990) (finding that the physician's staff privileges did not make the hospital vulnerable to respondeat superior liability for his actions).

86. Mduba v. Benedictine Hosp., 384 N.Y.S.2d 527, 529 (N.Y. App. Div. 1976) (finding that a physician was a hospital employee rather than an independent contractor because the hospital controlled the way he operated its emergency room); *see generally* Martin C. McWilliams, Jr. & Hamilton E. Russell III, *Hospital Liability for Torts of Independent Contractor Physicians*, 47 S.C. L. REV. 431 (1996).

87. *See* Simmons v. St. Clair Mem'l Hosp., 481 A.2d 870, 874 (Pa. Super. Ct. 1984).

88. *Id.*; Burless v. W. Va. Univ. Hosps., Inc., 601 S.E.2d 85, 95–96 (W. Va. 2004) (discussing ostensible agency theory and proof criteria).

89. *See* Torrence v. Kusminsky, 408 S.E.2d 684, 692 (W. Va. 1991) (stating that "where a hospital makes emergency room treatment available to serve the public as an integral part

Through corporate negligence or vicarious liability theories, health care entities could be held liable for injuries caused by equipment defects or by their employees' misuse of sophisticated technology. The remainder of this Part will focus largely on clinicians' use of EHR systems and the potential problems they might experience.

2. Clinician Liability

Use of EHR systems could generate negligence claims against providers for a variety of reasons. EHR system operation can be time-consuming and burdensome, and increased work demands could cause rushed physicians to make medical mistakes. Greater access to existing diagnostic data and economic pressures to avoid duplicating tests could lead to errors from inappropriate reliance on outdated or inadequate prior testing. Mistakes may also result from data entry errors. Clinicians may be faulted for ignoring critical prompts and alerts from decision support features. Furthermore, providers who do not thoughtfully handle communication tools such as e-mail and PHRs may face frustrated, anxious, and litigious patients. Finally, product defects that affect medication orders or alerts can cause serious harm to patients. This Section will carefully consider each of these potential liability sources.

a) Physician Time Constraints and Information Overload

The typical contemporary physician faces significant time pressures and extreme workload demands.[90] A common complaint is that EHR system use is time consuming and requires clinicians to process an impossible amount of information.[91] This challenge can lead to medical mistakes and liability exposure.

The average visit to a primary care physician lasts thirteen to eighteen minutes.[92] Doctors are not able to spend sufficient time with patients to

---

of its facilities, the hospital is estopped to deny that the physicians and other medical personnel on duty providing treatment are its agents" and that "[r]egardless of any contractual arrangements with so-called independent contractors, the hospital is liable to the injured patient for acts of malpractice committed in its emergency room, so long as the requisite proximate cause and damages are present").

90. *See infra* notes 92–97 and accompanying text.

91. *See infra* notes 100–04and accompanying text.

92. Andrew Gottschalk & Susan A. Flocke, *Time Spent in Face-to-Face Patient Care and Work Outside the Examination Room*, 3 ANNALS FAM. MED. 488, 491 (2005) (finding that the average time per patient was 13.3 minutes); Kimberly S. H. Yarnall et al., *Family Physicians as Team Leaders: "Time" to Share the Care*, PREVENTING CHRONIC DISEASE: HEALTH RES., PRAC., & POL'Y 1, 6, Apr. 2009, http://www.cdc.gov/pcd/issues/2009/apr/08_0023.htm (finding that the mean length for an acute care visit is 17.3 minutes, the mean for a chronic disease

provide the comprehensive preventive and chronic disease care that is recommended in clinical practice guidelines.[93] In addition, physicians spend up to forty-five percent of their time each day attending to tasks outside of the examination room, such as reviewing charts, completing forms, writing prescriptions, consulting colleagues, and answering staff inquiries.[94] In a 2008 survey of approximately 11,950 physicians, over forty percent indicated that they saw between twenty-one and thirty patients per day, and over seventy-five percent described their practices as either at "full capacity" or "overextended and overworked."[95] If these responses are representative,[96] most physicians would find it very difficult to accommodate additional work in their already crowded schedules.[97]

It is also unlikely that physicians will decrease the number of patients they see in order to address time pressures. The United States is facing a

---

care visit is 19.3 minutes, and the average for a preventive care visit is 21.4 minutes, and that of total clinical time spent by physicians, these comprise 45.8%, 37.4%, and 16.8% respectively); Kevin Fiscella & Ronald M. Epstein, *So Much to Do, So Little Time: Care for the Socially Disadvantaged and the 15-Minute Visit*, 168 ARCH. INTERNAL MED. 1843, 1843 (2008) ("The average office visit in the United States lasts for about 16 minutes."); Chen, *supra* note 11, at 329 (reporting that the average time spent by patients with providers during 1998–2008 was 16.4 minutes).

93. Fiscella, *supra* note 92, at 1843–44; Truls Østbye et al., *Is There Time for Management of Patients with Chronic Diseases in Primary Care?*, 3 ANNALS FAM. MED. 209, 212 (2005) ("We calculated that comprehensive high-quality management of 10 common chronic diseases require more time than primary care physicians have available for all patient care."); Yarnall et al., *supra* note 92, at 1 ("The common denominator in the failure to deliver services is probably lack of physician time."). For a discussion of clinical practice guidelines *see infra* Section IV.B.2.a).

94. Gottschalk & Flocke, *supra* note 92, at 490–91; Jeffrey Farber et al., *How Much Time Do Physicians Spend Providing Care Outside of Office Visits?*, 147 ANNALS INTERNAL MED. 693, 695–97 (2007).

95. THE PHYSICIANS' FOUNDATION, THE PHYSICIANS' PERSPECTIVE: MEDICAL PRACTICE IN 2008: SURVEY SUMMARY & ANALYSIS, 4 (2008), http://www.physicians foundations.org/usr_doc/PF_Survey_Report.pdf. More specifically, the number of patients per day seen by physicians was as follows: 7.4% saw 0–10; 31.71% saw 11–20; 41.28% saw 21–30; 13.68% saw 31–40; 3.71% saw 41–50; 0.99% saw 51–60, and 1.23% saw over 61. In describing their practices, 44.92% indicated that they were at full capacity; 31.37% were "overextended and overworked;" and 23.71% indicated that they "[h]ave time to see more patients and assume more duties." *See also* Gottschalk & Flocke, *supra* note 92, at 491 (finding that the "mean number of patients seen per day was 29.1" in a survey of eleven primary care physicians who did not use EHRs).

96. THE PHYSICIANS' FOUNDATION, *supra* note 95, at 4. A major limitation of the study is that the response rate was only four percent. *Id.* at 4. It is possible that the respondents are a self-selected group of individuals who felt particularly pressured or unhappy. Nevertheless, the report is based on answers from 11,950 physicians, which is not an insignificant number. *Id.*

97. Yarnall et al., *supra* note 92, at 1; Østbye et al., *supra* note 93, at 212.

shortage of primary care physicians,[98] so fewer doctors are available to treat a growing U.S. population. In addition, financial incentives discourage doctors from reducing the number of patients they see, and decreasing Medicare, Medicaid, and private insurance reimbursements may threaten the economic viability of some practices and require them to maintain a high volume of patient visits.[99]

EHR systems impose new demands on physicians' workdays.[100] They require clinicians to type text directly into the EHR, a task that is disfavored by some providers.[101] According to one study, using bedside or examination room computers increased physician documentation time by 17.5 percent while using centrally located desktops for CPOE rather than prescription pads increased physician documentation time by 98.1 percent to 328.6 percent.[102] Typing visit notes in accordance with EHR specifications generally takes longer than dictating notes or writing a succinct visit summary by hand.[103] EHR systems have templates that require physicians to record far more information than they have traditionally included in paper files, and not all of the information is essential or even relevant to proper patient care.[104]

---

98. THE PHYSICIANS' FOUNDATION, *supra* note 95, at 10 (reporting that 78% of physicians believe there is a shortage of primary care physicians); Kevin Grumbach & Thomas Bodenheimer, *A Primary Care Home for Americans: Putting the House in Order*, 288 J. AM. MED. ASS'N 889, 890 (2002) (stating that "primary care is endangered" because fewer medical school graduates are choosing to become primary care physicians and to practice internal medicine).

99. THE PHYSICIANS' FOUNDATION, *supra* note 95, at 3 (discussing declining Medicare and Medicaid reimbursement); Yarnall et al., *supra* note 92, at 1 (noting the problem of "inadequate insurance reimbursement"); Ming Tai-Seale et al., *Time Allocation in Primary Care Office Visits*, 42 HEALTH SERVS. RES. 1871, 1886 (2007) ("Incentives in prevailing physician payments favor procedure-based patient care over time-intensive evaluation and management care."); Leigh Ann Backer, *Strategies for Better Patient Flow and Cycle Time*, 9 FAM. PRAC. MGMT. 45 (2002), *available at* http://www.aafp.org/fpm/20020600/45stra.html (noting reduced Medicare and private insurance reimbursement and offering recommendations to maximize patient flow and cycle time in family medicine practices); Aris Sophocles, *Time Is of the Essence: Coding on the Basis of Time for Physician Services*, 10 FAM. PRAC. MGMT. 27, 27 (2003) (explaining that "CPT [current procedural terminology] lists a variety of codes that are strictly time dependent").

100. Thomas Bodenheimer, *Innovations in Primary Care in the United States*, 326 BRIT. MED. J. 796, 798 (2003) (asserting that EHR systems impose "extra demands on physicians' time").

101. C.R. Weir et al., *Direct Text Entry in Electronic Progress Notes*, 42 METHODS INF. MED. 61, 61 (2003).

102. Lise Poissant et al., *The Impact of Electronic Health Records on Time Efficiency of Physicians and Nurses: A Systematic Review*, 12 J. AM. MED. INFORMATICS ASS'N 505, 508 (2005).

103. Baron et al., *supra* note 14, at 225; Weir et al., *supra* note 101, at 66.

104. Weir et al., *supra* note 101, at 65 (noting that templates may be up to 5 pages in length); Anne Armstrong-Coben, *The Computer Will See You Now*, N.Y. TIMES, Mar. 5, 2009, at A27 (asserting that the EHR system requires her "to bring up questions in the order they

Time spent on EHR-related tasks is time not spent interacting directly with patients.[105] Physicians who have fewer minutes to speak with and examine patients may provide lower quality care. In addition, patients may resent the doctor's focus on the computer and apparent inattention to them[106] and be more apt to sue if they are dissatisfied with their health outcomes. This concern is not theoretical. Multiple studies have shown that patients most often decide to sue when they are displeased with the quality of the physician-patient relationship and feel they cannot communicate well with their doctors.[107]

Computerized records can be lengthy and cumbersome to read. Whereas having to write notes by hand encourages brevity, physicians entering notes electronically may copy large segments of information from elsewhere in the record for the sake of completeness.[108] But this practice may make it far more difficult for a provider to obtain an overview of the patient's current condition or locate a needed detail quickly.[109] With interoperability,[110] doctors may have access to records from patients' visits to numerous specialists and be expected to consider all relevant information concerning each patient's medical and treatment history.[111] The challenges of reviewing a patient's entire EHR may be compounded by data display problems. Doctors may need to scroll through numerous screens in order to find the detail they seek, information may be organized awkwardly or fragmented throughout the EHR, and all data might appear in a uniform format so that physicians seeking a particular fact cannot easily scan the data.[112]

The challenges posed by the large volumes of information contained in interoperable EHRs could be addressed in part through the work of nurses or other lower-cost providers who meet with the patient at the beginning of

---

appear [and] to ask the parents of a laughing 2-year-old if she is 'in pain' ").

105. Armstrong-Coben, *supra* note 104, at A27 (explaining that the computer interferes "with what should be going on in the exam room—making that crucial connection between doctor and patient").

106. Baron et al., *supra* note 14, at 224 (reporting that after EHR system implementation, some patients asked, "Doctor, do you find you are spending more time interacting with the computer than with your patients?").

107. Beth Huntington & Nettie Kuhn, *Communication Gaffes: A Root Cause of Malpractice Claims*, 16 BAYLOR U. MED. CENTER PROC. 157, 157–60 (2003) (reviewing studies that explore the circumstances in which patients decide to sue their physicians).

108. Weir et al., *supra* note 101, at 66.

109. Armstrong-Coben, *supra* note 104, at A27 ("In the past, I could pick up a chart and flip through it easily . . . . Now . . . important points often get lost.").

110. BIOMEDICAL INFORMATICS, *supra* note 12, at 952.

111. *See* Hoffman & Podgurski, *supra* note 13, at 112–13.

112. Ross Koppel, *Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors*, 293 J. Am. Med. Ass'n 1197, 1199–1201 (2005).

the appointment. These providers could review the EHR and interview the patient before the doctor enters the examination room and then supply the physician with notes or a verbal report summarizing and highlighting the most relevant information. This approach, while potentially helpful, would raise issues of vicarious liability for physicians. Under the doctrine of respondeat superior, doctors who directly supervise and control staff members may be held liable for injuries associated with inaccurate or deficient summary reports provided by office personnel.[113]

Case law establishes that physicians can be held liable for harm that could have been averted had they more carefully studied their patients' medical records. For example, *Short v. United States* involved a patient whose doctor failed to diagnose his prostate cancer in time for it to be cured.[114] The court held that under Vermont law, the physician violated the standard of care by failing to review the patient's past visit notes, which would have elucidated the nature of his condition.[115] In *Conrad-Hutsell v. Colturi*, a court of appeals reversed a directed verdict for the defendant.[116] The court held that a question of fact existed as to whether a physician, who did not obtain a copy of the patient's medical record that would have indicated a history of narcotics overuse, should be held liable for the patient's addiction to the drugs he prescribed.[117]

With EHR systems, clinicians may find it extremely difficult to process the plethora of information that floods their computer screens.[118] Yet those who miss a critical detail, such as a past illness treated by a different specialist that might affect the doctor's therapeutic decision, could be held liable for negligence because the fact in question was likely just a few clicks away when the physician was reviewing the patient's EHR.[119] The demands of EHR

113. Carol R. Goforth, *Limiting the Liability of General Partners in LLPs: An Analysis of Statutory Alternatives*, 75 OR. L. REV. 1139, 1201–13 (1996) (discussing the respondeat superior doctrine and its application to medical malpractice cases); Franklin v. Gupta, 567 A.2d 524, 537 (Md. Ct. Spec. App. 1990) (explaining that a physician can be held liable if "the negligent actors were, in fact, under his direct supervision and control"); Harris v. Miller, 438 S.E.2d 731, 741 (N.C. 1994) (holding that the defendant physician "enjoyed authoritative control" over a nurse anesthetist who performed his job duties negligently during surgery and that the trial court erred in "refusing to submit plaintiff's vicarious liability claim to the jury").

114. Short v. United States, 908 F. Supp. 227, 231–33 (D. Vt. 1995) (explaining that the patient required a bilateral orchiectomy and was not expected to survive for long).

115. *Id.* at 236.

116. No. L-01-1227, 2002 WL 1290844 (Ohio Ct. App. May 24, 2002).

117. *Id.* at 1–2.

118. Armstrong-Coben, *supra* note 104, at A27 (stating that EHRs present "screens filled with clicked boxes," that all information is provided in the same font, and that "important points often get lost").

119. EHR systems may also make discovery more burdensome and complicated than it

system operation and the very large amounts of information that users could be expected to consider may thus lead to malpractice liability.

b) Reliance on Others' Diagnosis and Treatment Decisions

Interoperability could raise another malpractice challenge as well by providing clinicians with incentives to rely on prior tests results. Currently, patients who transfer to a new doctor or seek a second opinion may be subjected to the same battery of tests that they have already undergone elsewhere.[120] With interoperability, authorized clinicians will have direct access to the results of all prior diagnostic tests and procedures, no matter where they were conducted. In light of "government and private studies [that] have found that much of the $2.5 trillion spent on health care each year

---

was in the past. Rule 34 of the Federal Rules of Civil Procedure allows parties to request to inspect, copy, test, or sample any electronically stored information, including e-mail, image files, and material from databases. Furthermore, the producing party must present the requested data in a reasonably usable form. FED. R. CIV. P. 34 (a)–(b).

EHRs may be difficult to produce and review because they are voluminous, especially if they are interoperable and contain records from all of the patient's treating physicians, laboratories, radiologists, and other providers. In addition, their format might make them abstruse to those not carefully trained in the system because of fragmented displays and other usability problems. EHRs may also generate unique authentication problems. User access, computer programming changes, backup systems, inputs, and other aspects of EHR system operation must all be carefully controlled in order to safeguard the integrity and authenticity of all medical records. Kevin Brady et al., *E-Discovery in Healthcare & Pharmaceutical Litigation: What's Ahead for ESI, PHI & EHR?*, 9 SEDONA CONF. 167, 174–75 (2008). In addition, the integrity of EHRs could be compromised during the discovery process itself because of inappropriate search and retrieval procedures, data conversion or other forms of mishandling. *Id.* at 174–75; *In re* Vinhee, 336 B.R. 437, 444 (9th Cir. 2005) (discussing authenticity and explaining that "the record being proffered must be shown to continue to be an accurate representation of the record that originally was created"). Thus, responding to document requests involving EHRs could be time-consuming, cumbersome, and costly. *See generally* Cecily Walters, *Attorney Survey Reveals Concerns About Litigation* Costs, TRIAL, Feb. 2009, at 64 (reporting that in responding to a survey of fellows of the American College of Trial Lawyers, "more than 87 percent said that e-discovery increases litigation costs, and almost 77 percent indicated that courts 'do not understand the difficulties in providing e-discovery.' "). *But see* Thomas R. McLean, *EMR Metadata Uses and E-Discovery*, 18 ANNALS HEALTH L. 75, 109 (2009) (explaining that because medical malpractice actions often require only the records of one patient or a few patients, the volume of documents involved in e-discovery may not be significantly greater than the amount involved in "traditional paper discovery").

120. CONG. BUDGET OFFICE, EVIDENCE ON THE COSTS AND BENEFITS OF HEALTH INFORMATION TECHNOLOGY 11 (2008), *available at* http://www.cbo.gov/ftpdocs/91xx/doc9168/05-20-HealthIT.pdf (discussing the potential for duplicated testing); Jan Walker et al., *The Value of Health Care Information Exchange and Interoperability*, HEALTH AFF., Jan. 19, 2005, at W5-10, W5-13-14, http://content.healthaffairs.org/cgi/content/full/hlthaff.w5.10/DC1 (discussing redundant testing).

is wasted on the duplication of tests and unneeded procedures,"[121] providers will likely be under considerable pressure to avoid repeating tests in order to achieve cost savings.[122] However, reliance on prior test results can lead to misdiagnoses or sub-optimal treatment decisions. For example, a technician who was sloppy or not sufficiently skilled may have conducted the prior test, or the patient's condition could have changed in the intervening time.[123]

One study of one hundred cases involving diagnostic errors determined that eight were caused by "[o]verreliance on someone else's finding or opinion" and failure to verify other clinicians' diagnoses in light of current findings.[124] Such mistakes have led to litigation and large plaintiff recoveries. For example, in *Whitaker v. Frankford Hospital*, a patient suffered a massive stroke after being discharged by an emergency room doctor who relied on a radiologist's interpretation of an MRA/MRI that erroneously indicated only a "very low percentage of blockage" in the carotid arteries.[125] Both physicians were among the defendants, and the plaintiff ultimately recovered millions of dollars through a settlement with some defendants and a jury verdict against others.[126] Because interoperable EHR systems would provide easy access to previously gathered medical data, problematic reliance on other clinicians' findings may become increasingly common.[127]

---

121. Robert O'Harrow Jr., *The Machinery Behind Health-Care Reform*, WASHINGTONPOST.COM, May 16, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/05/15/AR2009051503667.html (suggesting that EHR systems could diminish the waste generated by the duplication of tests).

122. *Id.*; CONG. BUDGET OFFICE, *supra* note 120, at 11 (discussing the avoidance of duplicate or inappropriate diagnostic tests); Rainu Kaushal et al., *Return on Investment for a Computerized Physician Order Entry System*, 13 J. AM. MED. INFORMATICS ASS'N 261, 263 tbl. 1 (2006) (discussing the financial benefits of EHR systems, including decreased laboratory tests and radiology utilization); Walker et al., *supra* note 120, at W5-16 ("Interoperability between . . . organizations would enable computer-assisted reduction of redundant tests.").

123. R. James Brenner et al., *Radiology and Medical Malpractice Claims: A Report on the Practice Standards Claims Survey of the Physician Insurers Association of America and the American College of Radiology*, 171 AM. J. ROENTGENOLOGY 19, 20–21 (1998) (discussing the association between diagnostic errors and poor image quality in various radiological tests); E. James Potchen & Mark A. Bisesi, *When Is It Malpractice to Miss Lung Cancer on Chest Radiographs?*, 175 RADIOLOGY 29, 30 (1990) (stating that "poor image quality alone may be a source of negligence").

124. Mark L. Graber et al., *Diagnostic Error in Internal Medicine*, 165 ARCHIVES INTERNAL MED. 1493, 1497 (2005).

125. Nos. 1557, 2007 Phila. Ct. Com. Pl. LEXIS 287, at *2 (Pa. C.P. 2007).

126. *Id.* at *1–4.

127. It should be noted, however, that in some cases, conducting repeated tests is not in the patient's best interest. This would be true if the initial results are accurate, and the test is very uncomfortable or exposes the patient to risk such as radiation, or if the second diagnostic procedure shows different, incorrect results upon which the doctor may erroneously rely.

Physicians will thus face difficult decisions regarding whether to re-order expensive tests to verify diagnoses. They will need to continue to balance the competing interests of patient welfare, liability risks, and cost savings.

c) Input Errors

While paper files may contain illegible handwriting, misspellings, or other errors, use of automated technology may exacerbate the problem of record inaccuracies.[128] A study of sixty patient records with 1,891 notes from the Department of Veterans Health Administration's Computerized Patient Record System (CPRS) found that eighty-four percent of notes contained "at least one documentation error," and there were an average of 7.8 documentation mistakes per patient.[129] For example, cut and paste functions are designed to save doctors time by allowing them to copy information from old clinical notes into new progress notes. If such notes are not carefully edited, old symptoms, vital signs, or test results can appear to be current, and such mistakes can create new threats to patient safety and liability exposure for clinicians.[130]

A number of other problems can also arise because of careless clinician data entry. Occasionally, notes are entered into the wrong patient's record, and such erroneous information may mislead subsequent providers who consult an EHR.[131] In one reported incident, an "AIDS patient was wrongly told he had skin cancer on his neck because a test result for another patient was associated with his electronic record."[132] Likewise, physicians may hit the wrong key or inadvertently read the wrong patient's electronic record and thus base a treatment decision on incorrect information. In addition, users utilizing electronic signatures often neglect to indicate their titles or credentials.[133] This omission could be significant in a hospital setting, where

128. Weir et al., *supra* note 101, at 61.

129. *Id.* at 62, 64.

130. *Id.* at 64–65; Kenric W. Hammond et al., *Are Electronic Medical Records Trustworthy? Observations on Copying, Pasting and Duplication*, AMIA 2003 SYMP. PROC. 269, 269, 272 (2003), *available at* http://www.pubmedcentral.nih.gov/picrender.fcgi?artid=1480345&blobtype=pdf (reviewing 243 VA patient files and finding that 9% of notes contained copied text); Eugenia L. Siegler & Ronald Adelman, *Copy and Paste: A Remediable Hazard of Electronic Health Records*, 122 AM. J. MED. 495, 495–96 (2009) (cautioning that cut and paste functions can lead to patient problem lists never changing, notes and errors being copied by multiple staff members, and loss of accurate narrative).

131. Weir et al., *supra* note 101, at 65 (finding five instances out of 1,891 in which narrative notes were typed for the wrong patient).

132. Jacob Goldstein, *Big Challenges Await Health-Records Transition*, WALL ST. J., April 21, 2009, at A4.

133. Weir et al., *supra* note 101, at 65 (finding that 53% of electronic signatures "failed to appropriately reflect the credentials and/or title of the author").

care coordinators need to determine whether a patient was visited by a particular type of clinician or whether a specific treatment decision was made at the appropriate authority level.

Providers' reliance on electronic systems to order medication and other treatments is another novel source of medical mistakes.[134] One study of a hospital's CPOE system found that it posed the following challenges, which could lead to incorrect user input and consequent dosage errors:

> (1) Cumbersome medication charting and fragmented displays make it difficult to identify the patient to whom a particular record belongs or require doctors to look at numerous screens in order to obtain the patient's full medication list;
>
> (2) Physicians may fail to enter discontinuation orders for particular drugs when they change patients' medications so that the pharmacy continues to provide the old drugs as well as the new ones;
>
> (3) Problematic log-off procedures cause physicians to order medications on the system before the previous user has fully logged out, resulting in the wrong patient receiving the newly-ordered therapy;
>
> (4) The system requires that drug orders be reactivated rather than automatically transferred when patients are moved within the hospital (e.g. from the intensive care unit to a regular hospital room) so that patients whose doctors fail to reactivate orders are deprived of needed medications; and
>
> (5) System inflexibilities significantly impede providers' ability to enter nonstandard specifications or to order non-formulary medications.[135]

Medication errors and other mistakes involving CPOE functionality could thus lead to medical malpractice litigation and physician liability if they harm patients.

d) The Challenges of Decision Support

Decision support, defined as "any information added by a system to assist the clinician's decision-making process,"[136] can come in many forms.

---

134. Joan S. Ash et al., *Some Unintended Consequences of Information Technology in Health Care: The Nature of Patient Care Information System-Related Errors*, 11 J. AM. MED. INFORMATICS ASS'N 104, 106 (2004) (discussing errors relating to entering and retrieving information as well as communication and coordination problems).

135. Koppel, *supra* note 112, at 1199–1201. Non-formulary medications are "[d]rugs not on a [health care] plan-approved drug list." Medicare Glossary Definitions, http://www.medicare.gov/Glossary/search.asp?SelectAlphabet=N&Language=English#Content.

136. Handler et al., *supra* note 25, at 1135.

These include prompts based on clinical practice guidelines, clinical alert systems that warn providers about problems such as drug allergies and drug interactions, data tags that elucidate test results (such as an "L" next to a low laboratory value), and recommendations for diagnostic tests and treatment modalities based on patients' symptoms and conditions.[137] Although decision support has the potential to improve the quality of health care, it can also be disruptive in some circumstances. Furthermore, evidence that a doctor ignored automated alerts or recommendations may serve as compelling proof of physician wrongdoing for plaintiffs who suffer poor outcomes because of a doctor's treatment decision.

Studies have shown that decision support can appreciably improve patient care. One study found that reminders can significantly increase the use of preventive measures such as pneumococcal and influenza vaccinations in hospitalized patients.[138] Several other articles confirm the usefulness of decision support for preventive care purposes.[139]

Other researchers, however, have found that decision support is frequently disregarded.[140] According to one article, physicians often ignored suggestions concerning disease management because they distrusted them, did not appreciate a computer telling them how to practice medicine, or were too busy to consider computerized recommendations carefully.[141] Another study found that physicians did not follow suggestions because they could be

137. *Id.* at 1135–36.

138. 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) (stating that with reminders, the use of pneumococcal vaccination increased from approximately zero to approximately 35%, and the use of influenza vaccinations increased from approximately zero to approximately 50% in the hospital).

139. Clement J. McDonald et al., *The Regenstrief Medical Record System: a quarter century experience*, 54 INT'L J. MED. INFORMATICS 225, 247 (1999) (asserting that "[r]eminders increased the use of preventive interventions up to four-fold," including use of influenza vaccines, mammography, and cervical pap testing); Alex R. Kemper et al., *Adoption of Electronic Health Records in Primary Care Pediatric Practices*, 118 PEDIATRICS e20, e23 (2006) (stating that "[a]lthough prompts for preventive services can improve care, many of the EHRs in use do not provide this feature").

140. Amit X. Garg et al., *Effects of Computerized Clinical Decision Support Systems on Practitioner Performance and Patient Outcomes*, 293 J. AM. MED. ASS'N 1223, 1231 (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 25, at 1136 (stating that the benefit of decision support during documentation is unclear and often does not seem to affect clinicians' adherence to recommended guidelines).

141. 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 (2003).

erased without being read if the user hit the escape key.[142] However, when the escape key was disabled, provider adherence to suggestions increased significantly.[143] Some postulate that providers might be resistant to decision support concerning disease management but receptive to suggestions concerning preventive care,[144] which may be perceived as less challenging to their professional judgment.

At times, it is medically appropriate for doctors to discount decision support messages. In many instances, decision support prompts and alerts can be excessive and disruptive and, therefore, justifiably overridden.[145] For example, drug-allergy alerts often indicate merely that some patients are sensitive to the medication even though they will suffer no serious reaction, and alerts continue to appear even if the patient has tolerated a medication well.[146] Drug-allergy alerts often do not distinguish between warnings of high clinical significance and the much more routine notices of benign drug sensitivities, so that all alerts are provided in the same format and color.[147] Researchers have found that doctors accept fewer than twenty percent of drug-allergy alerts, and almost all overrides are medically appropriate and do not risk significant harm to patients.[148] However, a doctor who is accustomed

142. William M. Tierney, *Can Computer-Generated Evidence-Based Care Suggestions Enhance Evidence-Based Management of Asthma and Chronic Obstructive Pulmonary Disease? A Randomized, Controlled Trial*, 40 HEALTH SERVS. RES. 477, 491 (2005).

143. Dexter et al., *supra* note 138, at 968.

144. Subramanian et al., *supra* note 141, at 379; Tierney, *supra* note 142, at 491–92; INSTITUTE OF MEDICINE, CROSSING THE QUALITY CHASM: A NEW HEALTH SYSTEM FOR THE 21ST CENTURY (2001). (finding convincing evidence that decision support improves preventive care, patient monitoring, and appropriate drug prescriptions but a dearth of convincing evidence for its usefulness for diagnosis and disease management).

145. Saeid Eslami et al., *Evaluation of Outpatient Computerized Physician Medication Order Entry Systems: A Systematic Review*, 14 J. AM. MED. INFORMATICS ASS'N 400, 404 (2007). (concluding that alerts are "largely ignored by physicians" but that many "alerts are not applicable to the patient at hand" or "are not clinically important"); Gilad J. Kuperman et al., *Medication-related Clinical Decision Support in Computerized Provider Order Entry Systems: A Review*, 14 J. AM. MED. INFORMATICS ASS'N 29, 30 (2007) ("Excessive drug-allergy alerting in clinically irrelevant circumstances is highly prevalent and a major disruptor of clinicians' workflows.").

146. Kuperman et al., *supra* note 145, at 404.

147. *Id.*

148. *Id.* (citing Susan A. Abookire et al., *Improving Allergy Alerting in a Computerized Physician Order Entry System*, PROC. AM. MED. INFORMATICS ASS'N SYMP. 2, 2–6 (2000), *available at* http://www2.amia.org/pubs/symposia/D200703.PDF; Tyken C. Hsieh, *Characteristics and Consequences of Drug Allergy Alert Overrides in a Computerized Physician Order Entry System*, 11 J. AM. MED. INFORMATICS ASS'N 482 (2004).

to overriding alerts may become desensitized to them and occasionally ignore a critical one.[149]

Yet despite such practices, proof that a physician overrode or ignored an alert may constitute powerful evidence of wrongdoing for injured plaintiffs in litigation. In *Jones v. Bick*, the court found that a doctor failed to meet the standard of care when he did not consider warnings contained in the Physicians' Desk Reference (PDR) concerning the anti-psychotic drug prescribed to a patient who subsequently died of cardiac arrest.[150] It is even more likely that a physician would be found liable in similar circumstances if he did not have to use a reference book such as the PDR, but rather had a warning appear on his computer screen.

Like physicians, health care entities can be sued for ignoring CPOE warnings. Already, several pharmacies have been sued for failing to contact physicians to inform them of prescription problems of which they were made aware by electronic alerts. In *Cafarelle v. Brockton Oaks CVS, Inc.*, the court denied summary judgment to a pharmacy that overrode warning prompts and filled a child's Proventil inhaler prescriptions three times more often than was appropriate.[151] *In Happel v. Wal-Mart Stores*, the court found that the pharmacy had a duty to warn the patient's physician that the drug he prescribed was contraindicated for his patient because she was allergic to aspirin.[152] The store routinely entered patients' allergy information into its computer and had allergy warnings appear when prescriptions were filled.[153] These are likely the first of many cases involving CPOE.

Decision support is designed to help clinicians achieve optimal outcomes. However, it may at times be disruptive and distracting, and it could create records of prompts and alerts that increase the risk of liability for health care providers.

---

149. Peter A. Gross & David W. Bates, *A Pragmatic Approach to Implementing Best Practices for Clinical Decision Support Systems in Computerized Provider Order Entry Systems*, 14 J. AM. MED. INFORMATICS ASS'N 25, 26 (2007) (speculating that users might "ignore the most critical interaction alerts due to 'information overload' or 'inability to recognize the needle in the haystack' ").

150. Jones v. Bick, 891 So. 2d 737, 746 (4th Cir. 2004); *see also* Fournet v. Roule-Graham, 783 So. 2d 439 (5th Cir. 2001) (affirming judgment for plaintiff who accused her physician of negligence based on his prescribing Provera despite a warning in the PDR that the drug should not be given to a patient with a history of deep vein thrombosis).

151. Cafarelle v. Brockton Oaks CVS, Inc., 5 Mass. L. Rep. 257, 257 (1996).

152. Happel v. Wal-Mart Stores, Inc., 766 N.E.2d 1118, 1121, 1125, 1128 (Ill. 2002).

153. *Id.*

e) Responsiveness to Electronic Communication

EHR systems may allow patients to communicate with physicians through secure messaging that authenticates recipients and encrypts text.[154] Such communication, however, can lead to further liability concerns if doctors do not instruct patients to avoid e-mail use when immediate care is necessary and do not limit patient expectations concerning this service. Electronic communication can increase clinicians' accessibility and decrease the need for telephone calls and ambulatory care visits as clinicians address patients' health concerns through e-mail.[155] Early evidence reveals a high level of patient satisfaction with e-mail communication.[156] Nevertheless, online messaging creates a new setting in which physicians must avoid mistakes or risk liability.[157] Doctors must determine whether to ask the patient to come to the office for a physical examination or to offer medical advice without an in-person visit. Similarly, doctors or their staff members must check e-mail

154. Chen et al., *supra* note 11, at 325 (describing Kaiser Permanente Hawaii's My Health Manager, a secure patient-physician messaging system through which members sent over 51,000 messages in 2007); Steven E. Waldren, *Email in Clinical Care*, 4 BMJ USA E325, E325 (2004), *available at* http://www.bmj.com/cgi/reprint/329/7471/E325 ("To ensure confidentiality, the recipient (patient) must be authenticated and the message itself must be transmitted in an encrypted manner.").

155. Chen et al., *supra* note 11, at 327 (finding a 26.2% percent reduction in the yearly total office appointment over 2004–2007, with face-to-face contact replaced by scheduled telephone visits and secure messaging); Madhavi R. Patt et al., *Doctors Who Are Using E-mail with Their Patients: A Qualitative Exploration*, J. MED. INTERNET RES. Apr.-Jun. 2003, http://www.jmir.org/2003/2/e9/ (stating that some physicians believed that e-mail would increase their accessibility to patients); Paul Rosen & C. Kent Kwoh, *Patient-Physician E-mail: An Opportunity to Transform Pediatric Health Care Delivery*, 120 PEDIATRICS 701, 704 (2007) (reporting that it took physicians 57% less time to respond to e-mail than to answer telephone calls); Yi Yvonne Zhou et al., *Patient Access to an Electronic Health Record with Secure Messaging: Impact on Primary Care Utilization*, 13 AM. J. MANAGED CARE 418, 424 (2007) (concluding that patients using electronic messaging had 6.7% to 9.7% fewer outpatient primary care visits than others). *Contra* Steven J. Katz et al., *Effect of a Triage-Based E-mail System on Clinic Resource Use and Patient and Physician Satisfaction in Primary Care*, 18 J. GEN. INTERNAL MED. 736, 742 (2003) (finding that "e-mail volume did not appear to offset phone volume or visit no-show rates").

156. Chen et al., *supra* note 11, 331–32 (reporting that 85% of patients "rated their satisfaction as 8 or 9 on a nine-point scale" and 85% felt that e-mail contact with physicians "enabled them to better manage their health"); Rosen, *supra* note 155, at 705–06 (reporting that families commented that e-mail "is one method of improving communication and providing consumer-driven health care"); Zhou et al., *supra* note 155, at 418 (reporting that 90% of patients with Internet access have a preference for electronic communication with providers).

157. Patt et al., *supra* note 155 (stating that doctors are concerned about e-mails reaching them in a timely fashion); Rosen, *supra* note 155, at 705 (stating that e-mail communication might produce anxiety about increased liability).

frequently enough so that patients are not neglected if the condition about which they are inquiring is serious.[158]

Physicians have been sued successfully for failing to respond to patient communication outside of office visits. In *St. Charles v. Kender*, the court held that an HMO patient had a viable breach of contract claim against a physician who failed to return her phone calls within two days, during which she suffered a miscarriage.[159] Likewise, in *Fletcher v. Ford*, an appellate court affirmed the denial of a doctor's summary judgment motion after he was sued for medical malpractice arising from his failure to return a telephone call that might have saved the life of an infant with meningitis.[160] By extension, plaintiffs might prevail in medical malpractice claims based on clinicians' unresponsiveness to e-mail.

Doctors may be alarmed by a Physician Insurers Association of America report revealing that $71.8 million in indemnity payments were made for 786 telephone-related malpractice claims.[161] A subsequent study of thirty-two telephone-related cases by malpractice insurers confirmed that such cases are costly and that patient injuries can be catastrophic.[162] Representative mistakes included flawed documentation of calls, inappropriate triage because of inadequate information obtained over the phone, and mismanagement of multiple calls made by the same patient.[163] Similar problems and shortcomings could easily arise when clinicians respond to patient e-mails.[164]

---

158. *See* Eric M. Liederman et al., *Patient-Physician Web Messaging*, 20 J. GEN. INTERNAL MED. 52, 52 (2005) (stating that physicians worry about being "overwhelmed by patient e-mails," that liability may arise because of missed diagnoses or delayed treatment, and that patients are dissatisfied with their physicians' response times). This study at the University of California Davis Health System found that 52.6% of "initial responses were sent within 4 business hours; 70.2% within 8 hours; and 85.5% within 16 hours." *Id.* at 54; *see infra* notes 313–16 for recommendations concerning physician-patient electronic communication.

159. 646 N.E.2d 411, 413 (Mass. App. Ct. 1995).

160. 377 S.E.2d 206, 207, 209 (Ga. Ct. App. 1988).

161. Harvey P. Katz et al., *Patient Safety and Telephone Medicine*, 23 J. GEN. INTERNAL MED. 517, 517 (2007).

162. *Id.* at 517.

163. *Id.* at 518–19; *see also* David E. Hildebrandt et al., *Harm Resulting from Inappropriate Telephone Triage in Primary Care*, 19 J. AM. BOARD FAM. MED. 437, 440–41 (2006) (finding that 1% of patients who called their doctors after hours suffered "harm or discomfort"); Barton D. Schmitt, *Telephone Triage Liability: Protecting Your Patients and Your Practice from Harm*, 55 ADVANCES IN PEDIATRICS 29, 31 (2008) (discussing delayed referral to medical care and other errors that occur in the after-hour call process); Bauer v. Mem'l Hosp., 879 N.E.2d 478, 490–91, 505 (Ill. App. Ct. 2007) (affirming the award of damages to plaintiffs for injuries suffered by an infant in part because his mother received inappropriate medical advice over the telephone).

164. *See infra* notes 313–15 for suggested e-mail protocols that could reduce liability risks.

f) Patient Access to PHRs

In addition to having secure messaging ability, patients may have PHRs that enable them to view part or all of their medical records.[165] However, while patients will likely appreciate such unprecedented access to their health data,[166] certain information might cause confusion, resentment, or trauma, and thus have an adverse health impact.

Providers establishing PHRs must decide whether to include the patient's entire problem, medication and allergy lists, laboratory and diagnostic test results, and comprehensive clinical notes.[167] Some commentators are concerned that if providers share candid psychiatric problem lists and complete progress notes, including personal impressions, patients could become less cooperative with or trusting of their doctors.[168] In the alternative, providers could tailor their notes to avoid causing discomfort to PHR readers, but this approach might sacrifice accuracy.[169]

Also, patients who receive bad news through electronically transmitted test results rather than through a conversation with a sensitive clinician could be traumatized, misunderstand their diagnoses, or feel angry or hopeless.[170] Such patients might decide to stop complying with their treatments and suffer clinical setbacks. Plaintiffs with poor outcomes who feel that their doctors were uncommunicative or insensitive in their communication may be more likely than others to sue.[171] Thus, physicians' decisions to post or omit certain information from PHRs could contribute to the likelihood of medical malpractice claims against them.

---

165. *See supra* notes 53–62 and accompanying text.

166. MARKLE FOUNDATION, ATTITUDES OF AMERICANS REGARDING PERSONAL HEALTH RECORDS AND NATIONWIDE ELECTRONIC HEALTH INFORMATION EXCHANGE (2005), http://www.phrconference.org/assets/research_release_101105.pdf (finding that 60% of Americans support the creation of secure PHRs, and only 19% of Americans state they would not use PHRs for any purpose).

167. Halamka, *supra* note 54, at 3–5.

168. *Id.*

169. It should be noted that the HIPAA Privacy Rule allows patients access to their medical records. Specifically, the regulations provide that "an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set," with some exceptions, such as psychotherapy notes and information compiled for purposes of litigation or administrative proceedings. Furthermore, the Privacy Rule enables individuals to request amendment of PHI that is incorrect. 45 C.F.R. §§ 164.524, 164.526(a) (2008). These provisions, however, would not require doctors to include any specific information in a PHR.

170. Halamka, *supra* note 54, at 4 (reporting that at the authors' institution, all results are released to patients immediately except for HIV results, cytology/pathology results, and results from MRI/CT testing done to follow cancer progression).

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

Yet another concern relates to patients' ability to add notes and information to their PHRs.[172] Patients might wrongly assume that they are communicating directly with their doctors by inputting data and expect physicians to review their PHR entries regularly. Doctors would be well-advised to ask patients using PHRs to sign a form that explains the extent to which clinicians will review this submitted data, if at all. Without such a notice, patients who are harmed because their doctors ignored or never saw important details that they noted in their PHRs may file malpractice claims.

g) Product Defects

In some cases, EHR systems themselves or the computing platforms that support them will be flawed.[173] Thus, EHR system use can cause poor outcomes because of product defects rather than user error. In early 2009, the public learned that software glitches in the Veterans Affairs' EHR system exposed veterans to potentially life-threatening drug dosage errors, including excessively prolonged intravenous infusion of the blood-thinner heparin.[174] Other such instances include flawed EHR system software that provided erroneous calculation of intracranial pressure[175] and a case in which ninety-three minutes of data were missing from the automated anesthesia record of a brain tumor patient who woke up from surgery as a quadriplegic.[176]

CPOE systems have been particularly vulnerable to criticism. While some of their weaknesses lead to input errors,[177] they are also susceptible to software defects. These include: (1) incorrect prompts regarding dosages; (2) an absence of warnings that drug orders must be renewed or that certain drug combinations are inappropriate; (3) failure to automatically cancel medication orders when procedures that require the drugs are cancelled or postponed; (4) lack of interoperability and communication among different systems within the same hospital, such as those belonging to the pharmacy

172. *See supra* notes 58–61 and accompanying text.

173. Jonathan K. Gable, *An Overview of the Legal Liabilities Facing Manufacturers of Medical Information Systems*, 5 QUINNIPIAC HEALTH L.J. 127, 129–31 (2001) (describing instances in which improper medical treatment was provided because of computer programming or software errors); Ross Koppel & David Kreda, *Health Care Information Technology Vendors' "Hold Harmless" Clause: Implications for Patients and Clinicians*, 301 J. AM. MED. ASS'N 1276, 1278 (2009) ("[I]n many cases, HIT problems may be caused not by clinicians but by poor software.").

174. Yen, *supra* note 16.

175. Koppel & Kreda, *supra* note 173, at 1276.

176. Michael M. Vigoda & David A. Lubarsky, *Failure To Recognize Loss of Incoming Data in an Anesthesia Record-Keeping System May Have Increased Medical Liability*, 102 ANESTHESIA & ANALGESIA 1798, 1798–99 (2006).

177. *See supra* note 141–42 and accompanying text.

and house staff; and (5) computer crashes and maintenance shutdowns that lead to lost orders.[178]

One review found that information inconsistencies in CPOE systems pose significant risks to patient safety.[179] Information inconsistencies were defined as disparities between data entered through structured templates and information in free-text comment fields.[180] The review examined 55,992 CPOE prescriptions and concluded that 532 of them contained errors, most commonly in dosage, of which twenty percent could have caused moderate to significant harm.[181] Errors were attributable to automated dosage defaults, comments automatically transferred to new prescriptions after modification of existing prescriptions, insufficient training on CPOE systems, and flawed standardized templates.[182]

Both health care organizations and physicians can be held liable for harms associated with use of faulty equipment. Hospitals, clinics, or physicians who purchase low-quality, defective EHR systems or fail to maintain the systems properly could be sued for any resulting harm suffered by patients.[183] Whether or not a decision to adopt a particular product constitutes negligence will depend on professional custom.[184] If providers select an EHR system that is widely recognized as inadequate, and the system causes injury to patients, plaintiffs might be able to establish medical malpractice.[185]

It is also possible that physicians who did not participate in their employer's decision to choose a defective EHR system could be found liable for negligence because of product flaws. While many physicians will not have the technical expertise to detect certain software defects, in some cases they

178. Koppel, *supra* note 112, at 1199–1201.

179. Hardeep Singh et al., *Prescription Errors and Outcomes Related to Inconsistent Information Transmitted Through Computerized Order Entry*, 169 ARCHIVES INTERNAL MED. 982, 989 (2009).

180. *Id.* at 983.

181. *Id.* at 984, 986.

182. *Id.* at 987–88.

183. Lamb v. Candler Gen. Hosp., 413 S.E.2d 720, 721–22 (Ga. 1992) ("It is well recognized that a hospital may be liable in ordinary negligence for furnishing defective equipment for use by physicians and surgeons in treating patients."); Berg v. United States, 806 F.2d 978, 983 (10th Cir. 1986) (upholding a verdict for the plaintiff whose injuries were caused in part by a lack of adequate testing and maintenance of equipment and a lack of adequate training of technicians).

184. *See supra* notes 73–74 and accompanying text.

185. *See* Emory Univ. v. Porter, 120 S.E.2d 668, 670 (Ga. Ct. App. 1961) (stating that a hospital has a "duty of exercising ordinary care to furnish equipment and facilities reasonably suited to the uses intended and such as are in general use under the same, or similar, circumstances in hospitals in the area").

may become aware of system flaws that generate obvious errors. A physician who used an EHR system knowing that it caused particular problems such as dosage errors, who did not demand that her employer ensure that the system is repaired, and who took no precautions, such as reviewing each dosage recommendation to ensure accuracy, might be deemed by a court to be responsible for patient injuries. In *Wickline v. State of California*, a California court of appeals stated in dicta that "the physician who complies without protest with the limitations [of covered hospitalization days] imposed by a third party payer, when his medical judgment dictates otherwise, cannot avoid his ultimate responsibility for his patient's care."[186] Thus, if a court finds that a reasonable physician would not have tolerated her institution's faulty EHR system without protest and without implementing clinical safeguards to avoid patient harm, the individual might be held liable in a medical malpractice case.

Contractual provisions favored by EHR vendors may exacerbate the liability vulnerability of clinicians using EHR systems. Vendors may disclaim implied and express warranties or insert "hold harmless" clauses into their contracts that shield them from liability and shift responsibility for harm to health care providers.[187] Contractual provisions that limit liability can be invalidated as violating public policy if the parties have unequal bargaining power or the provision encourages reckless or negligent behavior.[188] Thus, courts may find "hold harmless" provisions unenforceable if they are convinced that health care providers lack the technical knowledge and sophistication to bargain on equal footing with vendors.[189] Judges may also revoke provisions that are deemed likely to promote carelessness on the part

186. 192 Cal. App. 3d 1630, 1645 (1986). In this case, a doctor sought permission from Medi-Cal to extend his patient's hospital stay by eight days. An extension was granted for only four days, and the doctor released the patient at the end of that period. The patient was later readmitted to the hospital because of complications, and her leg had to be amputated. She sued the state of California, which operated Medi-Cal, but the court of appeals ultimately found that the state was not liable for Wickline's injuries.

187. Koppel & Kreda, *supra* note 173, at 1276; Lisa L. Dahm, *Restatement (Second) of Torts Section 324A: An Innovative Theory of Recovery for Patients Injured Through Use or Misuse of Health Care Information Systems*, 14 J. MARSHALL J. COMPUTER & INFO. L. 73, 78, 92–93 (1995); Gable, *supra* note 173, at 141.

188. Blake D. Morant, *Contracts Limiting Liability: A Paradox with Tacit Solutions*, 69 TULANE L. REV. 715, 734 (1995); Tunkl v. Regents of the Univ. of Cal., 383 P.2d 441, 447 (Cal. 1963) (finding that a hold harmless agreement imposed as a condition of admission to a hospital was invalid because the patient had unequal bargaining power); Emory Univ. v. Porubiansky, 282 S.E.2d 903, 904–06 (Ga. 1981) (holding that a waiver of claims in an informed consent agreement was invalid as a matter of public policy).

189. Koppel & Kreda, *supra* note 173, at 1276 (arguing that there exists a "substantial disparity between buyers and sellers in knowledge and resources").

of manufacturers.[190] In the alternative, states may enact statutes that invalidate particular types of hold harmless clauses.[191] Typically, however, contractual limitations of liability are enforceable.[192]

B. PRIVACY BREACHES

Computerized information is vulnerable to large-scale privacy violations associated with hacking, computer theft, malicious electronic distribution, or accidental disclosure, such as sending a file to the wrong e-mail address.[193] Once data security is breached, the most private information can be dispersed on the Internet to a worldwide audience.[194] Disclosure of psychiatric or sexual histories or other sensitive information can, among other harms, lead to profound embarrassment, ruined careers, or loss of professional and personal opportunities.[195] These, in turn, can generate litigation against those responsible for security breaches.

1. Security Threats and Regulation

Privacy breaches involving EHRs have occurred in the United States with alarming frequency. For example, in 2008, computer files containing health and financial details of more than 2.1 million patients were stolen from a storage company hired by the University of Miami Health System, and information about 6,000 patients of the University of California San Francisco Medical Center was available online for three months.[196] That same year, a laptop belonging to a National Institutes of Health researcher was stolen, compromising private information about nearly 2,500 heart disease patients.[197] According to some estimates, between 250,000 and 500,000 patients suffer medical identity theft each year.[198]

---

190. *Id.* (describing software malfunctions).

191. Carl Giesler, *Managers of Medicine: The Interplay Between MCOs, Quality of Care, and Tort Reform*, 6 TEX. WESLEYAN L. REV. 31, 50 (1999) (reporting that some states enacted statutes that invalidate hold-harmless clauses in contracts between physicians and managed care organizations).

192. Adloo v. H.T. Brown Real Estate, Inc., 686 A.2d 298, 301 (Md. 1995) ("It is well settled in this State, consistent with 'the public policy of freedom of contract,' . . . that exculpatory contractual clauses generally are valid.").

193. Hoffman & Podgurski, *In Sickness, Health and Cyberspace: Protecting the Security of Electronic Private Health Information*, *supra* note 30, at 333.

194. *Id.* at 335.

195. *Id.* at 334–35.

196. American Medical Association, *News in Brief: Miami Patient Data Stolen*, AM. MED. NEWS, May 19, 2008, http://www.ama-assn.org/amednews/2008/05/19/bibf0519.htm.

197. *Safeguarding Private Medical Data*, N.Y. TIMES, March 26, 2008, at A22. In 2006 an Aetna laptop computer containing personal information concerning 38,000 consumers was stolen and a security breach compromised the confidentiality of records from 60,000 patients

To address the threats to patient privacy, the U.S. Department of Health and Human Services (HHS) enacted the Privacy Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[199] The Privacy Rule requires health care providers to safeguard patient privacy in a variety of ways. For example, with some exceptions, covered entities must obtain a patient's permission before speaking to third parties about the patient's medical condition;[200] must distribute privacy notices containing information concerning use and disclosure of patients' health records;[201] and must allow patients to inspect their health records and request that they be modified or used restrictively.[202] The HIPAA Security Rule, which is part of the Privacy Rule, focuses specifically on data security and the electronic storage and transmission of private health information (PHI).[203] The Security Rule, which became effective on April 20, 2005 for most covered entities,[204] delineates administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information.[205]

Despite the regulatory mandates, many commentators agree that privacy and security threats still abound. A large 2007 study of security vulnerabilities concluded that "commercial EHR systems are vulnerable to exploitation given existing industry development and disclosure practices."[206] A 2008 report issued by the HHS Office of the Inspector General concluded that the

---

who visited Ohio University's health center. *See* Ronald A. Williams, *Statement of Aetna CEO and President Ronald A. Williams on Data Security*, Apr. 6, 2006, http://www.aetna.com/news/2006/pr_20060426.htm; Jennifer Gonzalez, *3rd Computer Breach at OU Within 3 Weeks*, THE PLAIN DEALER, May 12, 2006, at A1.

198. Judith Graham, *Medical Identity Theft Spreads: Purloined Data Often the Crime of Insiders*, CHI. TRIB., Aug. 22, 2008, at 10.

199. The HIPAA Privacy Rule is found at 45 C.F.R. §§ 160.101–164.534 (2008). HIPAA provides statutory authority for these regulations at 42 U.S.C. §§ 1320d–1320d-8 (2006).

200. 45 C.F.R. § 164.510 (2008).

201. 45 C.F.R. § 164.520(a) (2008).

202. 45 C.F.R. §§ 164.520, 164.522 (2008).

203. 45 C.F.R. §§ 164.302–164.318 (2008). Under the Privacy Rule, PHI includes "individually identifiable health information" that is electronically or otherwise transmitted or maintained. 45 C.F.R. § 160.103 (2008).

204. 45 C.F.R. § 164.318 (2008). Small health plans were given an extended adjustment period and were required to comply with the rule by April 20, 2006.

205. For a description and critique of the HIPAA Security Rule, see Hoffman & Podgurski, *In Sickness, Health and Cyberspace: Protecting the Security of Electronic Private Health Information*, *supra* note 30.

206. *eHVRP Study Finds Healthcare Industry Must Do More to Protect Electronic Health Record Systems*, BUS. WIRE, Sept. 17, 2007, *available at* http://www.thefreelibrary.com/_/print/PrintArticle.aspx?id=168732503. The study was conducted over 15 months and surveyed more than 850 provider organizations.

federal government had failed to provide adequate oversight or effective enforcement of the HIPAA Security Rule.[207] Preliminary results of HHS audits of U.S. hospitals revealed "numerous, significant vulnerabilities" in PHI protections that jeopardize its confidentiality.[208]

PHRs may raise particular privacy challenges. Web-based PHRs enable the service provider to obtain and sell health information to marketers and advertisers.[209] Employers who offer PHRs to workers[210] might be tempted to retrieve data and use it for purposes of employment decisions.[211] Those designing PHRs must incorporate safeguards to ensure that patients or their authorized proxies are properly authenticated before accessing their PHRs and that all others are blocked from doing so.[212]

The threats to EHR security have not eluded public notice. When asked, the overwhelming majority of American patients express concern about the privacy of their medical records. A 2005 National Consumer Health Privacy Survey involving 2,000 individuals revealed that sixty-seven percent of respondents were "somewhat" or "very concerned" about PHI confidentiality.[213] Furthermore, thirteen percent of respondents claimed that they had attempted to protect their own privacy by avoiding medical tests or visits to their regular physicians, asking doctors to distort diagnoses, or paying for tests out-of-pocket so that no medical documentation would be sent to insurance companies.[214] That same year, a Markle Foundation survey found that "[a]ttributes of a proposed nationwide health information exchange that focus on security and privacy are rated as the highest priorities among survey respondents."[215] In a 2007 online survey, forty percent of respondents disagreed with the statement that "the benefits of electronic medical records outweigh the privacy risks."[216]

---

207. DANIEL R. LEVINSON, DEP'T OF HEALTH AND HUMAN SERVS., NATIONWIDE REVIEW OF THE CENTERS FOR MEDICARE & MEDICAID SERVICES HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 OVERSIGHT, A-04-07-05064, 3 (2008), *available at* http://www.oig.hhs.gov/oas/reports/region4/40705064.pdf.

208. *Id.* at 3–4.

209. Terry, *supra* note 21, at 237.

210. *See* Halamka et al., *supra* note 54 and accompanying text.

211. DANIEL R. LEVINSON, *supra* note 207, at 3–4.

212. Halamka et al., *supra* note 54, at 5.

213. LYNNE "SAM" BISHOP ET AL., CAL. HEALTHCARE FOUND., NATIONAL CONSUMER HEALTH PRIVACY SURVEY 2005, at 3 (2005).

214. *Id.* at 4.

215. MARKLE FOUNDATION, *supra* note 166, at 2.

216. Robert Steinbrook, *Personally Controlled Online Health Data—The Next Big Thing in Medical Care?*, 358 N. ENGL. J. MED. 1653, 1655 (2008).

2. Potential Litigation

Patients who learn that their medical information has been inappropriately disclosed to third parties may be inclined to sue their physicians. Litigation may be facilitated by the HITECH Act, which includes several provisions designed to enhance the efficacy of the HIPAA Privacy and Security Rules.[217] The law requires that covered entities[218] notify individuals of any security breaches[219] involving their "unsecured" PHI.[220] Thus, if providers comply with this mandate, patients will learn of security breaches that compromise their PHI. In fact, patients might initiate litigation not only when the physician has carelessly or intentionally disclosed PHI, but also when the disclosure occurred because of hacking or an EHR system defect. It will be up to courts to determine whether providers are at fault for such security breaches.[221]

Patients could sue clinicians for privacy breaches under a variety of theories. The tort of invasion of privacy is one possibility. It consists of four elements: (1) public disclosure; (2) of a private fact; (3) that would be objectionable and offensive to a reasonable person; and (4) that is not of

---

217. *See* Reece Hirsch & Rebecca Fayed, *ARRA 2009 and the HITECH Act: The Next Phase of HIPAA Regulation and Enforcement Arrives*, 18 BNA'S HEALTH L. REP. 308 (2009) (detailing the law's privacy-related provisions).

218. Covered entities are health plans, health care clearinghouses, and health care providers who transmit health information electronically for claims, billing or health plan purposes. 45 C.F.R. § 160.103 (2008). The HITECH Act establishes that the Security Rule's requirements also apply to business associates of covered entities. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13401, 123 Stat. 115, 260 (2009) (to be codified at 42 U.S.C. § 17931(a)).

219. The term "breach" is defined as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13400(1)(A), 123 Stat. 115, 258 (2009) (to be codified at 42 U.S.C. § 17921). For exceptions to this definition, see § 13400(1)(B).

220. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13402(a), 123 Stat. 115, 260 (2009) (to be codified at 42 U.S.C. § 17932(a)). Unsecured PHI is to be defined through DHHS guidance, but if the Secretary fails to issue guidance, it will be defined as "PHI that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute." American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13402(h)(1)(B)–(h)(2), 123 Stat. 115, 262–63 (2009) (to be codified at 42 U.S.C. § 17932(h)(1)(B)–(h)(2)).

221. *See supra* note 186 and accompanying text.

legitimate public concern.[222] An alternative tort theory is breach of confidentiality,[223] whose elements are (1) the existence of a doctor-patient relationship, and (2) a physician's or medical entity's disclosure to a third party of confidential information that was gained pursuant to this relationship.[224]

State law can provide plaintiffs with additional causes of action.[225] For example, the California Constitution explicitly establishes that state residents

---

222. *See* Diaz v. Oakland Tribune, 188 Cal. Rptr. 762, 766 (Ct. App. 1983) (reporting that the jury found defendant liable for publicizing the fact that plaintiff had gender-corrective surgery).

223. Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 652–58 (2002) (discussing the common law tort theory of breach of confidentiality and its implications).

224. Sorensen v. Barbuto, 143 P.3d 295, 299 (Utah Ct. App. 2006) (discussing claim of breach of confidentiality where physician communicated with party opposing patient while litigation was pending); Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999) (establishing that "in Ohio, an independent tort exists for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship"); Kimberly Rathbone, *The Strict Ohio Supreme Court Decisions in* Biddle*: Third Party Law Firm Held Liable for Inducing Disclosure of Medical Information*, 15 J.L. & HEALTH 189, 196–97 (2001).

225. Some states provide aggrieved parties with a general cause of action for privacy breaches. *See* CAL. CIV. CODE §§ 56.35–56.36 (2008); MD. CODE ANN., HEALTH-GEN. § 4-309(f) (2009); MASS. GEN. LAWS ANN. CH. 214 § 1B (2005); MINN. STAT. ANN. § 144.298 (2005 & SUPP. 2009); MONT. CODE. ANN. § 50-16-553 (2007), *amended by* 2009 Mont. Laws 56 (to be codified at MONT. CODE ANN. § 13-15-205); N.H. REV. STAT. ANN. § 151:30 (2009); TENN. CODE ANN. § 68-11-1504 (2009); TEX. HEALTH & SAFETY CODE ANN. § 241.156 (Vernon 2001); TEX. OCC. CODE ANN. § 159.009 (Vernon 2004); WASH. REV. CODE ANN. § 70.02.170 (2009) *amended by* 2009 Wash. Sess. Laws page no. 1493; WYO. STAT. ANN. § 35-2-616 (2009).

Other states provide a more limited cause of action for improper disclosure of specific medical information such as HIV/AIDS test results, genetic testing, and mental health records. Statutes relating to HIV/AIDS are: ARIZ. REV. STAT. ANN. § 36-668 (2009); CAL. HEALTH & SAFETY CODE § 120980 (2009); CONN. GEN. STAT. ANN. § 19a-590 (2003 & Supp. 2009); DEL. CODE ANN. tit. 16, § 1205 (2009); 410 ILL. COMP. STAT. ANN. 305/13 (2005 & Supp. 2009); IOWA CODE § 141A.11 (2005 & Supp. 2009); ME. REV. STAT. ANN. tit. 22, § 825 (2004 & Supp. 2009); ME. REV. STAT. ANN. tit. 5, § 19206 (2009); MICH. COMP. LAWS § 333.5131(8) (2001); MO. REV. STAT. § 191.656(6) (2004 & Supp. 2009); MONT. CODE. ANN. § 50-16-1013 (2007), *amended by* 2009 Mont. Laws 362; N.H. STAT. ANN. § 141-F:10 (2009); N.D. CENT. CODE § 23-07.5-07 (2008); OKLA. STAT. tit. 63, § 1-502.2(H) (2004 & Supp. 2009) *amended by* S.B. 928, 52nd Leg., 1st Reg. Sess. (Okla. 2009); 35 PA. CONS. STAT. § 7610 (2003); TEX. HEALTH & SAFETY CODE ANN. § 81.104 (Vernon 2009); VA. CODE ANN. § 32.1-36.1(c) (2009); WASH. REV. CODE ANN. § 70.24.084 (2002); W. VA. CODE ANN. § 16-3C-5 (2006).

Litigation rights for disclosure of mental health information are provided by: CAL. WELF. & INST. CODE § 5330 (1998 & Supp. 2009); 740 ILL. COMP. STAT. 110/15 (2002 & Supp. 2009); TEX. HEALTH & SAFETY CODE ANN. § 611.005 (Vernon 2009 & Supp. 2009); WASH. REV. CODE ANN. § 71.05.440 (2008); WISC. STAT. ANN. § 51.30 (2008 & Supp.

have a right to privacy,[226] and the California Confidential Medical Information Act (CMIA) generally prohibits health care providers from disclosing their patients' records without their authorization.[227] In *Kina v. United Air Lines Inc.*, a federal district court allowed a plaintiff to proceed with his claim that his state constitutional and statutory rights were violated when his "fitness-for-duty" exam results were disclosed to his employer without his authorization.[228] Similarly, in *Berger v. Sonneland*,[229] the Supreme Court of Washington ruled that a statutory cause of action existed for a physician's unauthorized disclosure of a patient's medical information to her former husband.[230]

Although the HIPAA Privacy Rule does not provide aggrieved individuals with a private cause of action,[231] it might constitute evidence of the appropriate standard of care in negligence actions involving privacy breaches.[232] Furthermore, the HIPAA Privacy Rule authorizes government enforcement action for regulatory violations.[233] Providers may be subject to monetary penalties, with the amount depending on the severity of the offense.[234] Furthermore, the HITECH Act allows state attorneys general to bring civil actions for HIPAA violations in federal court.[235] The combination of federal investigations and litigation by attorneys general may subject providers to vigorous enforcement of the HIPAA Privacy Rule.

2009). Private action for disclosure of genetic information is allowed by: DEL. CODE ANN. tit. 16, § 1227(c) (2009); 410 ILL. COMP. STAT. ANN. 513/40 (2005 & Supp. 2009); MASS. GEN. LAWS ANN. ch. 111, § 706(d) (2003); NEV. REV. STAT. ANN. § 629.201 (2008); N.H. REV. STAT. ANN. § 141-H:6 (2009); N.J. STAT. ANN. § 10:5-49 (2002); N.M. STAT. ANN. § 24-21-6 (2009).

226. CAL. CONST. art. I, § 1.

227. CAL. CIV. CODE § 56.10(a) (2008) ("No provider of health care, health care service plan, or contractor shall disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c).").

228. 2008 WL 5071045, at *8–10 (N.D. Cal. Dec. 1, 2008).

229. 26 P.3d 257, 265 (Wash. 2001) (finding the disclosure to constitute "injuries occurring as a result of health care" under the statute).

230. *Id.* at 259, 269.

231. 45 C.F.R. §§ 160.300–160.552 (2008); Hoffman & Podgurski, *supra* note 30, at 354.

232. Acosta v. Byrum, 638 S.E.2d 246, 253 (N.C. Ct. App. 2006) (explaining that HIPAA was relevant to the extent it provided evidence of the duty of care owed by a physician with respect to the privacy of a patient's medical records).

233. 45 C.F.R. §§ 160.300–160.552 (2008).

234. American Reinvestment and Recovery Act of 2009, Pub. L. No. 111-5, § 13410(d), 123 Stat. 115 (2009) (to be codified at 42 U.S.C. § 1320d-5).

235. *Id.*

C. DISCIPLINARY ACTION BY STATE MEDICAL BOARDS AND CRIMINAL PROSECUTION

The HIPAA Privacy Rule is not the only basis for government intervention with respect to provider misconduct. In egregious cases, health care professionals may also face disciplinary action by state medical boards, criminal prosecution for negligent or reckless treatment of patients, or other penalties.[236]

State Medical Practice Acts empower state medical boards to impose fines, reprimands, censures, probation, suspension, or license restriction or revocation on physicians who engage in misconduct.[237] Doctors who deviate unacceptably from the appropriate standard of care may be disciplined even if no individual patient was placed at risk or suffered tangible harm.[238] A particularly relevant example is *Bogdan v. New York State Board for Professional Medical Conduct*, in which the board imposed a two-year limited probation on an anesthesiologist, in part because of her failure to maintain adequate medical records.[239]

In addition, in extreme cases, physicians can be charged with involuntary manslaughter, negligent homicide, reckless endangerment, reckless homicide, grossly negligent medical care, or other criminal violations.[240] To illustrate, in *People v. Einaugler*, a doctor was convicted of reckless endangerment and willful violation of health laws after he failed to transfer a patient from a nursing-home to a hospital in a timely fashion.[241] In *Commonwealth v. Youngkin*,

---

236. Timothy J. Aspinwall, *Representing Healthcare Professionals in Disciplinary Actions: Containing the Collateral Damage*, 20 No. 3 HEALTH LAWYER 1, 1–6 (2008) (describing a variety of penalties that could be imposed on physicians providing substandard care); Ronald L. Eisenberg & Leonard Berlin, *When Does Malpractice Become Manslaughter?*, 179 AM. J. ROENTGENOLOGY 331, 332 (2002) (noting an increase in the criminal prosecution of physicians for reckless endangerment of patients); Laura J. Spencer, *The Florida "Three Strikes Rule" for Medical Malpractice Claims: Using a Clear and Convincing Evidence Standard to Tighten the Strike Zone for Physician Licensure Revocation*, 28 ST. LOUIS U. PUB. L. REV. 317, 321–24 (2008) (describing disciplinary proceedings by state medical boards).

237. Spencer, *supra* note 236, at 321, 327; James Morrison & Peter Wickersham, *Physicians Disciplined by a State Medical Board*, 279 J. AM. MED. ASS'N 1889, 1890, 1893 (1998) (reporting that in California, approximately 250 physicians are disciplined each year and estimating that 2400 physicians are disciplined each year in the United States).

238. Haw v. State Bd. of Med., 90 P.3d 902, 908 (Idaho 2004); Bogdan v. State Bd. for Prof'l Med. Conduct, 606 N.Y.S.2d 381, 382 (N.Y. App. Div. 1993).

239. *Bogdan*, 606 N.Y.S.2d at 382–83.

240. Paul R. Van Grunsven, *Medical Malpractice or Criminal Mistake? - An Analysis of Past and Current Criminal Prosecutions for Clinical Mistakes and Fatal Errors*, 2 DEPAUL J. HEALTH CARE L. 1, 14–43 (1997) (describing various criminal prosecutions).

241. 618 N.Y.S.2d 414, 414–15 (N.Y. App. Div. 1994).

a physician was convicted of involuntary manslaughter after the death of a seventeen year old patient to whom he prescribed a barbiturate.[242]

Physicians accused of providing substandard care may face other adverse consequences as well. They may lose their medical malpractice insurance, have their medical staff privileges suspended, or see their specialty board certification revoked.[243]

In the future, state board disciplinary proceedings, criminal prosecutions, or other penalties may be initiated because of performance deficiencies that are related to EHR systems. Health care professionals who rely improperly on prior physicians' diagnostic work, fail to review a patient's entire EHR, input data incorrectly, disregard prompts and alerts, or mishandle patient e-mail could face not only private medical malpractice lawsuits, but also governmental intervention.

IV. ADDRESSING LIABILITY RISKS: STRATEGIES AND RECOMMENDATIONS

Litigation and government enforcement actions offer retrospective review of challenged activities and provide post-hoc remedies to aggrieved parties. However, because lives are at stake in the health care setting, it is critical that prospective strategies be available to prevent patient harm before it occurs. We now turn to a variety of initiatives that may be undertaken to optimize EHR systems' effectiveness, maximize their usability for clinicians, and minimize risks to patient safety.

The medical community is at a crossroads. New health information technology has the potential to produce dramatic improvements in health outcomes. However, without safeguards, this technology could impair the performance of health care providers and expose them to unprecedented liability risks. We focus on two strategies to minimize these risks. First, EHR systems must be carefully regulated so that they cannot be marketed without being scrutinized, approved, and subject to ongoing oversight. Second, EHR system experts, clinicians, and the government should develop high-quality clinical practice guidelines and agency guidance concerning EHR systems. Such guidance will educate health care providers about proper EHR system acquisition and use practices and elucidate the standard of care for purposes of litigation.

---

242. 427 A.2d 1356, 1358–59, 1370 (Pa. Super. Ct. 1981).

243. *See* Aspinwall, *supra* note 236, at 5–6; William B. Schwartz & Daniel N. Mendelson, *Physicians Who Have Lost Their Malpractice Insurance: Their Demographic Characteristics and the Surplus-Lines Companies That Insure Them*, 262 J. AM. MED. ASS'N 1335, 1335 (1989).

A. ACHIEVING QUALITY CONTROL

Arguably, innovation in the EHR system industry can only be stimulated if the technology remains unregulated.[244] Government intervention that imposes burdensome requirements could discourage small entrepreneurs from entering the market. However, allowing manufacturers to produce and sell EHR systems whose quality and safety is unregulated could be extremely dangerous for patients and providers.

Without government oversight and quality control, health care providers will risk investing billions of dollars in poorly designed systems that compromise rather than improve health outcomes. Once a practice purchases a system, enters patient records into it, and trains its staff, it is likely to retain it even if it is deficient, rather than incur the high cost of switching systems. Flawed systems that lead to medical errors and poor health outcomes will inevitably increase providers' vulnerability to liability in medical malpractice cases. Similarly, a lack of governmental oversight to ensure that clinicians receive up-to-date, high-quality training concerning EHR systems could contribute to liability exposure.

1. Government Regulations

EHR systems are not currently approved or inspected by any regulatory agency prior to marketing.[245] Rather, a private sector organization called the Certification Commission for Health Information Technology (CCHIT) has developed a voluntary certification process for EHR systems.[246] However, the CCHIT certification process inadequately safeguards the quality and integrity of these products.[247] The short duration of testing and its deficient rigor substantially weaken the certification's utility. All testing occurs during one day, and therefore, inspectors do not observe the system operating over time and in a variety of usage environments.[248] Furthermore, applicants can access testing scenarios and scripts on CCHIT's website prior to testing. Therefore, they are not required to ensure that their systems appropriately handle the variety of user actions that can actually occur in the field.[249]

---

244. *See* Hoffman & Podgurski, *supra* note 13, at 126 (discussing the absence of regulation for EHR systems).

245. *See id.*

246. Certification Commission for Health Information Technology, About the CCHIT, http://www.cchit.org/about (last visited Sept. 24, 2009).

247. *See* Hoffman & Podgurski, *supra* note 13, at 132–34; Blumenthal, *supra* note 4, at 1478 (stating that "[t]ightening the certification process is a critical early challenge" for the Office of the National Coordinator of Health Information Technology).

248. *Id.* (stating that "[t]his inspection takes a full day").

249. CERTIFICATION COMMISSION FOR HEALTH INFORMATION TECHNOLOGY,

The HITECH Act suggests that improved certification criteria must be implemented. Section 3004 calls for the federal adoption of an "initial set of standards, implementation specifications, and certification criteria" by December 31, 2009.[250] Such criteria will presumably go beyond those already used by CCHIT. However, the HITECH Act does not detail how these standards and criteria will be implemented and enforced or what role the government will play in doing so. In fact, the legislation states that adherence to the new requirements will generally be voluntary for private entities.[251] Thus, the Act leaves the important matters of determining the safety and efficacy of these devices ambiguous.

A relaxed approach to EHR system oversight is misguided and dangerous.[252] EHR systems will affect many aspects of patient care and are critical medical tools.[253] Appropriate oversight would protect not only patients, but also clinicians and health care organizations, who would be less likely to use flawed technology that causes patient injuries. While federal regulation would not preclude patients from suing for injuries associated with EHR systems,[254] they may well diminish the likelihood of provider liability by enhancing the quality of the equipment they operate.

PHYSICIAN'S GUIDE TO CCHIT CERTIFICATION 8 (2008), *available at* http://www.cchit.org/sites/all/files/CCHITPhysiciansGuide08.pdf ("The criteria and test scripts are published on the Commission's web site: www.cchit.org.").

250. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3004, 123 Stat. 115, 240 (2009) (to be codified at 42 U.S.C. § 300jj-14).

251. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3001(c)(5)(A), 123 Stat. 115, 232 (2009) (to be codified at 42 U.S.C. § 300jj-11(c)(5)(A)) (discussing the "voluntary certification of health information technology"); Pub. L. No. 111-5, § 3006(a)(1), 123 Stat. 115, 241 (2009) (to be codified at 42 U.S.C. § 300jj-16(a)(1)) (explaining that generally, nothing in the Act shall be construed "to require a private entity to adopt or comply with a standard or implementation specification adopted under [the Act]").

252. In prior work we have argued that EHR systems should be subject to regulatory approval and monitoring processes akin to those applying the highest levels of scrutiny to devices regulated by the Food and Drug Administration. *See* Hoffman & Podgurski, *supra* note 13, at 128–31. The full argument will not be repeated here. We also will not address the important question of which specific agency should be tasked with EHR system oversight. For discussion, see *id.* at 134–40. Rather, we refer to the regulating entity merely as HHS, since the responsible agency will most likely be an arm of this department. The HITECH Act establishes the Office of the National Coordinator for Health Information Technology within HHS. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3001(a), 123 Stat. 115, 230 (2009) (to be codified at 42 U.S.C. § 300jj-11(a)).

253. Hoffman & Podgurski, *supra* note 13, at 128–31.

254. *See* Wyeth v. Levine, 129 S.Ct. 1187, 1204 (2009) (holding that state law failure to warn claims are not preempted by the FDA's approval of a warning label pursuant to federal law).

A regulatory framework that required all EHR systems to be tested extensively and approved before they are marketed, as is the case for drugs and medical devices,[255] could establish design criteria that would maximize EHR system usability and reduce the likelihood of input or chart review errors and other mistakes. Regulations could mandate that EHR vendors employ a "best practices" standard, requiring vendors to make reasonable efforts to identify and employ best practices relating to hazard and risk analysis and mitigation, software development, validation, maintenance, security measures, and system integration and operation. The selected practices should be similar to those commonly used by other industry members, or should be clearly demonstrated to be superior to commonly used measures.[256]

In addition, the regulations should specify requirements for particular features. For the sake of brevity, just two examples of criteria that could impact clinician liability will be provided.[257] First, HHS could articulate standards for CPOE applications and other forms of clinical decision support to optimize their safety and efficacy.[258] Second, it could require vendors to comply with user interface design guidelines for all EHR systems[259] so customers switching to a new EHR product would not require a long training and adjustment period and tend initially to introduce errors into medical records. Such standardization would not necessarily stifle competition, especially if HHS oversight included a mechanism for timely approval of innovative user interface features that conflict with existing guidelines.

Imposing regulatory requirements for design specifications is not unprecedented. The HIPAA Security Rule includes security standards and implementation specifications for security safeguards.[260] Similarly, the HITECH Act contemplates the development of standards, implementation

---

255. *See* 21 C.F.R. § 7.3(f) (2008) (defining the jurisdiction of the Food and Drug Administration); *see generally* 21 C.F.R. §§ 1–1405.670 (2009) (food and drug regulations); *see also* Hoffman & Podgurski, *supra* note 13 at 134–38 (critiquing FDA regulation of devices).

256. Hoffman & Podgurski, *supra* note 13, at 151.

257. For further details, see Hoffman & Podgurski, *supra* note 13, at 150–62.

258. *See* Kuperman, *supra* note 145, at 37 (providing recommendations for CPOE application vendors and drug information knowledge-base vendors). For example, alerts could be differentiated by color, which would indicate the seriousness of the potential harm to patients.

259. This could be done once experts have sufficient experience with EHR systems to determine the design of an optimal user interface.

260. 45 C.F.R. §§ 164.302–.318 (2008). *But see* Hoffman & Podgurski, *supra* note 30, at 344–59 (critiquing the HIPAA Security Rule).

specifications, and certification criteria for EHR systems.[261] We urge that these take the form of detailed regulatory requirements that are mandatory for all EHR system vendors.[262]

Ongoing monitoring is also critical for quality control[263] and can affect clinician liability risks. Currently, some EHR system contracts prohibit users from disclosing product problems to others.[264] Such restrictions increase the risk of harm to patients and should be prohibited by law. Vendors should be required to submit adverse event accounts to HHS, and summary reports of these events should be posted on the agency's website.[265] Adverse events would include all system problems that are associated with a design or operational flaw rather than with user error. Such reports would educate potential purchasers about product defects or usability problems. They may also protect providers who face litigation by proving that a vendor[266] rather than clinician was at fault for an EHR system problem that caused a poor medical outcome.[267]

Finally, state governments could mandate training both with respect to the particular product that a clinician is using and with respect to general EHR system use practices. Comprehensive and effective training is essential to the success of EHR system implementation.[268] As of 2009, sixty-two state medical boards required clinicians to earn continuing medical education

261. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3003(b)(1)(A), 123 Stat. 115, 238 (2009) (to be codified at 42 U.S.C. § 300jj-13(b)(1)(A)).

262. *See* Pub. L. No. 111-5, Title XIII, §§ 3006, 13112, 123 Stat. 115, 241, 243 (2009) (to be codified at 42 U.S.C. §§ 300jj-16, 17902) (requiring compliance only from private entities that enter into contracts with the federal government).

263. Hoffman & Podgurski, *supra* note 13, at 147–50 (discussing the need for ongoing monitoring of EHR systems).

264. Koppel & Kreda, *supra* note 173, at 1278.

265. Hoffman & Podgurski, *supra* note 13, at 148. Postings should delete trade secret information, confidential commercial and financial information, patient information, and information about the identities of the users who reported the adverse events; *see* 21 C.F.R. § 803.9, 814.44(d) (2008) (discussing the Food and Drug Administration's posting of redacted adverse event reports for medical devices).

266. We use the term "vendor" broadly to refer to those who develop or modify EHR system software and to those who sell and install such systems.

267. *See infra* note 340 and accompanying text (discussing the relevance of user problem reports to establishing the standard of care for EHR system use in litigation).

268. Wanda L. Krum & Jack D. Latshaw, *Training*, *in* IMPLEMENTING AN ELECTRONIC HEALTH RECORD SYSTEM 60–66 (James M. Walker et al. eds. 2005) (discussing the importance of training and providing recommendations for development of a successful training program); Kevin Grumbach & James W. Mold, *A Health Care Cooperative Extension Service: Transforming Primary Care and Community Health*, 301 J. AM. MED. ASS'N 2589, 2589 (2009) (noting that many clinicians "have little or no technical assistance to deploy and maintain new practice improvements like EHRs").

(CME) credits for license re-registration.[269] Many states mandate that clinicians study particular subject-matter in CME courses, such as ethics or pain management.[270] Following this precedent, EHR system training should become a uniform requirement for licensing by all state boards. Because CME credits must be approved by the state, and a certain number must be earned every year or two in most states,[271] such oversight would ensure that clinicians receive updated training. The quality of training courses is important as well. The HITECH Act establishes a Health Information Technology Extension Program and Health Information Technology Regional Extension Centers.[272] These federally-sponsored entities could coordinate training courses to ensure that they include suitable content and are of high value.[273] Formal CME training should be supplemented by other forms of support and assistance offered by the Regional Extension Centers.[274]

2. Agency Guidance

Federal regulations can be supplemented by agency guidance that clarifies and explicates regulatory mandates.[275] Because guidance documents are often developed without the public notice and comment period that is required for federal regulations, they generally do not have the force of law. Rather, they provide needed interpretation, instruction, and policy directions for those enforcing the law and those who must comply with it.[276] Guidance

269. AMERICAN MEDICAL ASSOCIATION, STATE MEDICAL LICENSURE REQUIREMENTS AND STATISTICS 2009 (2009), *available at* http://www.ama-assn.org/ama1/pub/upload/mm/40/table16-2009.pdf. This number includes several Doctor of Osteopathic Medicine boards.

270. *Id.*

271. *Id.*

272. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3012(a), (c), 123 Stat. 115, 247 (2009) (to be codified at 42 U.S.C. § 300jj-32(a), (c)). The Health Information Technology Extension Program is to "provide health information technology assistance services to be carried out through" HHS. The Health Information Technology Regional Extension Centers are to "provide technical assistance and disseminate best practices and other information" to facilitate and promote EHR system use.

273. Pub. L. No. 111-5, § 3012(c)(3)(F), 123 Stat. 115, 249 (2009) (to be codified at 42 U.S.C. § 300jj-32(c)(3)(F)) (urging that instruction concerning EHR systems be integrated "into the initial and ongoing training of health professionals").

274. Pub. L. No. 111-5, § 3012(c), 123 Stat. 115, 248 (2009) (to be codified at 42 U.S.C. § 300jj-32(c)); Grumbach & Mold, *supra* note 268, at 2589–90 (emphasizing the importance of "individualized support" and "technical assistance in the application of EHRs").

275. Lars Noah, *The FDA's New Policy on Guidelines: Having Your Cake and Eating It Too*, 47 CATH. U. L. REV. 113, 122 (1997).

276. *Id.* at 125; Paul R. Noe & John D. Graham, *Reflections on Executive Order 13,422: Due Process and Management for Guidance Documents: Good Governance Long Overdue*, 25 YALE J. ON

documents allow agencies to explain complex or ambiguous regulations quickly and provide a flexible and evolving forum for educating and instructing the public.[277] Thus, guidance is essential to successful regulatory programs.[278]

HHS has already begun the process of producing guidance concerning the HITECH Act. It recently issued guidance on health data security, which identified encryption and destruction of private health information prior to product disposal as essential security tools.[279] Furthermore, the HITECH Act establishes the Health Information Technology Research Center[280] within HHS, which would likely play a key role in producing guidance. If regulations governed the design, approval, and monitoring of EHR systems, then HHS guidance could provide detailed instructions concerning issues such as decision support, data display, and adverse event reporting.

B. ESTABLISHING THE STANDARD OF CARE

Government regulations and guidance will also be useful for establishing the standard of care in medical malpractice cases. The key to successfully defending a malpractice lawsuit is establishing that the defendant met or exceeded the applicable standard of care.[281] Typically, expert testimony is the proof mechanism for the standard of care in malpractice litigation.[282] Both

---

REGS. 103, 108 (2008). Some are concerned that agencies use guidance to circumvent the procedural requirements for promulgating regulations and to avoid judicial review, though occasionally courts have found guidance to be ripe for review and required compliance with it. Appalachian Power Co. v. EPA, 208 F.3d 1015, 1020 (D.C. Cir. 2000) (stating that when guidance is issued, "[l]aw is made without notice and comment, without public participation, and without publication in the Federal Register or the Code of Federal Regulations"); Nina A. Mendelson, *Regulatory Beneficiaries and Informal Agency Policymaking*, 92 CORNELL L. REV. 397, 411 (2007); James Hunnicutt, *Another Reason to Reform the Federal Regulatory System: Agencies' Treating Nonlegislative Rules as Binding Law*, 41 B.C. L. REV. 153, 174 (1999).

277. Mendelson, *supra* note 276, at 408.

278. Noe & Graham, *supra* note 276, at 108; Noah, *supra* note 275, at 125.

279. Breach Notification for Unsecured Protected Health Information; Interim Final Rule, 74 Fed. Reg. 42740 (proposed Aug. 24, 2009) (to be codified at 45 C.F.R. pt. 160, 164).

280. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 3012, 123 Stat. 115, 247–50 (2009) (to be codified at 42 U.S.C. § 300jj-32). The purpose of the Center is to "provide technical assistance and develop or recognize best practices to support and accelerate" EHR system adoption and use.

281. *See supra* notes 70–74 and accompanying text.

282. William Meadow, *Operationalizing the Standard of Medical Care: Uses and Limitations of Epidemiology to Guide Expert Testimony in Medical Negligence Allegations*, 37 WAKE FOREST L. REV. 675, 676 (2002) (explaining that jurors are informed about the standard of care "through the testimony of medical expert witnesses" who testify "based upon their own experience, knowledge, and training").

plaintiffs and defendants can present experts to testify about liability and to conduct what some have called "the battle of the experts."[283]

Because EHR systems are an emerging technology that is deployed only to a limited extent,[284] identifying professional custom and the standard of care for their use could be particularly challenging. Nevertheless, the infancy of this industry also presents a unique opportunity to establish reliable and clear EHR system guidelines that will optimize their design, promote their responsible use by clinicians, maximize their utility, and facilitate identification of the standard of care by expert witnesses at trial.[285]

The standard of care for EHR system use could be elucidated not only through governmental requirements, but also through clinical practice guidelines developed by professional organizations. In addition, audit trails built into EHR systems could provide powerful evidence of practices employed by the reasonable clinician and facilitate the development of reliable clinical practice guidelines. Each of these data sources will be discussed below.

1. Regulations, Agency Guidance, and Certification as Evidence of Standard of Care

Federal regulations, agency guidance, and certification[286] can serve as limited evidence of the standard of care in negligence cases. Administrative regulations do not provide definitive proof of the standard of care but constitute relevant evidence of it.[287] A defendant who complied with regulatory requirements may be found negligent if a reasonable practitioner would implement additional precautions.[288] Nevertheless, regulatory compliance is admissible in court as exculpatory evidence for defendants.[289]

283. Mello, *supra* note 73, at 684.

284. *See supra* note 6 and accompanying text.

285. *See* Michelle M. Mello, *Using Statistical Evidence to Prove the Malpractice Standard of Care: Bridging Legal, Clinical, and Statistical Thinking*, 37 WAKE FOREST L. REV. 821, 821 (2002) ("Increasingly, there have been calls to supplement expert opinion testimony in medical malpractice cases with more objective empirical evidence of various kinds to establish the legal standard of care.").

286. *See supra* Section IV.A for discussion of federal regulations, guidance, and certification.

287. Distad v. Cubin, 663 P.2d 167, 176 (Wyo. 1981).

288. RESTATEMENT (SECOND) OF TORTS § 288C (1965).

289. Ashley W. Warren, *Compliance with Governmental Regulatory Standards: Is it Enough to Immunize a Defendant from Tort Liability?*, 49 BAYLOR L. REV. 763, 778 (1997); Richard C. Ausness, *The Case for a "Strong" Regulatory Compliance Defense*, 55 MD. L. REV. 1210, 1241 (1996).

Compliance with agency guidance and certification by well-respected bodies, such as the International Standards Organization, has also been found to have probative value in establishing the standard of care in some areas of the law.[290] Thus, HHS guidance would serve not only to enhance the quality of EHR system use, but also to bolster the defense in medical malpractice cases. Although we argue that CCHIT certification should be replaced by a rigorous regulatory process,[291] in the interim, certification by a recognized authority will likely assist defendants in proving that they have met the standard of care to the extent that they adopted an EHR system of appropriate quality.[292]

2. Clinical Practice Guidelines

Clinical practice guidelines (CPGs) can potentially both educate clinicians on how to optimize EHR system use and constitute evidence of the standard of care. Existing CPGs have been subject to harsh criticism in the past.[293] However, the early stages of development of EHR technology may offer a unique opportunity to formulate CPGs that are objective, sound, and reliable.

a) What are CPGs?

CPGs can be defined as "[s]ystematically developed statements to assist practitioner and patient decisions about appropriate health care for specific clinical circumstances."[294] CPGs relating to diagnostic and treatment practices have been developed by professional societies, such as the American Medical Association and other physician specialty boards; federal and state governmental entities, such as the Agency for Healthcare Research

290. Brandt v. Rokeby Realty Co., 97C-10-132-RFS, 2004 Del. Super. LEXIS 297, at *1, 13, 16 (Del. Super. Ct. Sept. 8, 2004) (stating that EPA guidelines may be "helpful" and constitute "evidence of a standard" though they do not establish a standard of care); John Hedley-Whyte & Debra R. Milamed, *Equipment Standards: History, Litigation, and Advice*, 230 ANNALS OF SURGERY 120, 124 (1999) ("Juries and judges are swayed to the side of the defense by the use of equipment that has been certified to the relevant standard."); Janice M. Hogan & Thomas E. Colonna, *Products Liability Implications of Reprocessing and Reuse of Single-Use Medical Devices*, 53 FOOD & DRUG L.J. 385, 396 (1998); Naomi Roht-Arriaza, *Shifting the Point of Regulation: The International Organization for Standardization and Global Lawmaking on Trade and the Environment*, 22 ECOLOGY L.Q. 479, 516–17 (1995).

291. *See supra* notes 245–52 (critiquing CCHIT and discussing potential alternatives).

292. *See supra* notes 183–86.

293. Mello, *supra* note 73, at 708–09; Hal R. Arkes & Cindy A. Schipani, *Medical Malpractice v. The Business Judgment Rule: Differences in Hindsight Bias*, 73 OR. L. REV. 587, 631–32 (1994).

294. BIOMEDICAL INFORMATICS, *supra* note 12, at 924.

and Quality (AHRQ);[295] and health care payers, including health maintenance organizations and health insurers.[296]

Both plaintiffs and defendants have utilized CPGs in litigation.[297] Courts may view CPGs as establishing a presumption of due care, or at least as evidence of a practice that is accepted by a "respectable" minority.[298] Kentucky state law offers health care providers an affirmative defense based on adherence to CPGs.[299] However, some guidelines include disclaimers, stating that they are only advisory in nature or offer broad parameters rather than specific protocols, and such language significantly diminishes their evidentiary value.[300] Furthermore, several commentators are critical of CPGs in general and argue that they should not constitute reliable evidence of the standard of care in medical malpractice actions.

b) A Critique of CPGs

Critics note that the proliferation of CPGs may make it impossible to discern a clear medical custom.[301] A website called National Guideline Clearinghouse features over 2400 CPGs.[302] CPGs vary in quality and may provide inconsistent guidance concerning treatment of the same condition.[303]

---

295. For information about AHRQ, *see* U. S. DEPARTMENT OF HEALTH & HUMAN SERVICES, AGENCY FOR HEALTHCARE RES. AND QUALITY, WHAT IS AHRQ? (2002), *available at* http://www.ahrq.gov/about/whatis.pdf.

296. Mello, *supra* note 73, at 650.

297. Mello, *supra* note 73, at 648, 668 (stating that "empirical evidence indicates that CPGs currently are being used both as exculpatory evidence (by physician defendants) and as inculpatory evidence (by plaintiffs)," though their use is infrequent); Carter L. Williams, *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, 498 (2004) (explaining that courts have allowed both plaintiffs and defendants to introduce CPGs as evidence in litigation).

298. FURROW ET AL., *supra* note 76, at 350.

299. *See id.* The Kentucky statute provision reads as follows:

> Any provider of medical services under this chapter who has followed the practice parameters or guidelines developed or adopted pursuant to this subsection shall be presumed to have met the appropriate legal standard of care in medical malpractice cases regardless of any unanticipated complication that may thereafter develop or be discovered.

KY. REV. STAT. ANN. § 342.035(8)(b) (2006). Florida, Maine, and Minnesota enacted similar provisions, but those were subsequently repealed. FLA. STAT. ANN. § 408.02 (2002 & Supp. 2007); ME. REV. STAT. ANN. Tit. 24 §§ 2971–2979 (West 2000); MINN. STAT. § 62J.34(3)(a) (2005).

300. FURROW ET AL., *supra* note 76, at 350.

301. *See* Mello, *supra* note 73, at 653–54; Williams, *supra* note 297, at 491–92 (2004).

302. National Guideline Clearinghouse, http://www.guideline.gov/browse/guideline_index.aspx (last visited July 27, 2009).

303. Williams, *supra* note 297, at 491–92 (asserting that the sheer number of CPGs hinders physicians and that they vary in quality).

Some will be written with particular agendas in mind.[304] For example, health care payers' CPGs may be designed in part to standardize cost-cutting strategies, such as ordering fewer diagnostic tests for particular symptoms or prescribing less-expensive medications.[305] By contrast, professional societies' CPGs may be partially motivated by a desire to safeguard their autonomy and combat the health care payers' competing guidelines.[306]

Even the most well-established CPGs are not uniformly incorporated into practice and have been shown to be followed by only a narrow majority of physicians.[307] Furthermore, CPGs that are not continuously updated may quickly become obsolete as medical knowledge and technology evolves.[308] Moreover, in order to maintain sufficient flexibility to apply to a broad range of patients, medical practices, and circumstances, CPGs are often worded in vague terms.[309] This is because, the more specific the guidelines are, the more likely they are to be inapplicable to particular circumstances.[310] However, their vagueness can diminish their value for clinicians who are seeking detailed guidance.

Finally, litigants may question whether CPGs intend to represent prevailing medical custom, or, instead, ideals that providers should strive to achieve.[311] If they are ideals rather than a reflection of common clinical practice, they may be inappropriate as evidence of what a reasonable practitioner should be expected to do in particular circumstances.[312]

c) The Opportunity Presented by an Emerging Technology

While CPGs for disease diagnosis and treatment are at times controversial, experts may have a unique opportunity to develop helpful and influential CPGs to guide EHR system use. Very few CPGs exist concerning health information technology, and if the tide of CPG proliferation can be

304. *Id.* at 492 (stating that "[p]otential conflicts of interest may . . . create significant credibility problems with CPGs").

305. *See* Mello, *supra* note 73, at 651.

306. *Id.* at 650–51.

307. *Id.* at 680–83 (asserting that a study of 143 guidelines showed a compliance rate of 54.5%); *see also* Mello, *Using Statistical Evidence to Prove the Malpractice Standard of Care: Bridging Legal, Clinical, and Statistical Thinking*, *supra* note 285, at 844 (arguing that compliance level that far exceeds 50% is required to establish custom).

308. *See* Williams, *supra* note 297, at 487; Arkes & Schipani, *supra* note 293, at 632.

309. *See* Mello, *supra* note 73, at 686–87.

310. Arkes & Schipani, *supra* note 293, at 631–32.

311. Mello, *supra* note 73, at 677; B. Michael Dann, *Jurors as Beneficiaries of Proposals to Objectify Proof of the Standard of Care in Medical Malpractice Cases*, 37 WAKE FOREST L. REV. 943, 949 (2002) (stating that CPGs are "more aspirational in nature than purely descriptive of actual practice").

312. Mello, *supra* note 73, at 677.

stemmed early on, many of the traditional shortcomings of CPGs could be avoided.

A literature search revealed only three U.S.-based CPGs regarding electronic communication between physicians and patients. In 1998, the American Medical Informatics Association (AMIA) developed "Guidelines for the Clinical Use of Electronic Mail with Patients."[313] The guidelines include the following recommendations, among others: (1) establish a specific turnaround time for communication; (2) inform patients about privacy matters, such as who might read messages and whether e-mail will be incorporated into the patient's medical record; (3) articulate what transactions are permitted over e-mail and specify that e-mail should not be sent about urgent matters; (4) ask patients to indicate the subject of the e-mail in the subject line (e.g., prescription, appointment, advice) to facilitate routing; (5) instruct patients to include their name and patient number in the message's text; (6) provide automatic replies to acknowledge receipt of e-mail; (7) inform patients through e-mail that their requests were completed; (8) ask patients to acknowledge reading clinicians' responses through autoreply; (9) word messages carefully to avoid insensitivity to patients and other communication problems; and (10) obtain patient informed consent for e-mail use that includes instructions, descriptions of security mechanisms, and indemnity provisions for providers.[314] The American Medical Association and the eRisk Working Group for Healthcare subsequently issued their own CPGs, which offer similar recommendations.[315]

Unfortunately, a study conducted several years after the AMIA guidelines were published revealed that, as is typical with other CPGs, only a minority of practices are adhering to the recommendations.[316] Nevertheless, as providers become more focused on liability associated with EHR system use,

313. Beverley Kane & Daniel Z. Sands, *Guidelines for the Clinical Use of Electronic Mail with Patients*, 5 J. AM. MED. INFORMATICS ASS'N 104 (1998).

314. *Id.* at 106–07.

315. AMERICAN MEDICAL ASSOCIATION, GUIDELINES FOR PHYSICIAN-PATIENT ELECTRONIC COMMUNICATIONS (2003), http://www.imageamerica.com/downloads/AMAGEC.pdf; ERISK WORKING GROUP, ERISK WORKING GROUP FOR HEALTHCARE'S GUIDELINES FOR ONLINE COMMUNICATION (2006), *available at* http://one.aao.org/asset.axd?ID=03e68ca0-e08e-4e3c-a227-16b0d0714872; *see also*, Amy M. Bovi, *Ethical Guidelines for Use of Electronic Mail Between Patients and Physicians*, 3 AM. J. BIOETHICS W43, W46 (2003); CAN. MED. ASS'N, PHYSICIAN GUIDELINES FOR ONLINE COMMUNICATION WITH PATIENTS (2005), http://oscarresourceplone.oscartools.org/it/pd05-03.pdf.

316. Robert G. Brooks & Nir Menachemi, *Physicians' Use of Email With Patients: Factors Influencing Electronic Communication and Adherence to Best Practices*, J. MED. INTERNET RES. e2 (2006) (finding that only 6.7% of doctors participating in a survey adhered to at least half of 13 selected guidelines).

they may be more motivated to adopt recommended safeguards. The AMIA CPGs and others of similar quality are particularly likely to be followed if they contain detailed, unambiguous suggestions that are not contradicted by conflicting guidelines. Thus, newly created EHR system CPGs that are formulated by well-respected authorities and widely adopted by physicians could serve the dual role of providing valuable guidance to clinicians and establishing professional custom for litigation purposes.

d) A Proposed Approach for CPG Development

CPGs could be developed through an open process and careful evaluation that is coordinated by a central organization. This process would be based on the demonstrably successful model used by the Internet Engineering Task Force (IETF)[317] to select the standards that underlie the operation of the Internet.[318] While federal regulations and guidance would address the initial approval and ongoing monitoring of EHR systems, clinical practice guidelines would provide recommendations concerning clinicians' use practices, such as e-mail communication, cutting and pasting, handling of drug alerts, chart review, and other functions.

The IETF is a technical standardization body, whose work is done by approximately 130 working groups.[319] These groups are open to any member of the public with appropriate expertise who is willing to make the necessary time commitment.[320] Working groups endorse documents through "rough consensus" rather than a formal vote, meaning that "a very large majority of those who care must agree."[321]

IETF standards begin as Internet drafts, which can be submitted by anyone and are distributed for public comments through IETF directories.[322] After sufficient discussion and revision, if the working group leaders believe

317. *See* Internet Engineering Task Force, http://www.ietf.org.

318. *See* Internet Engineering Task Force, *IETF Standards Process,* http://www.ietf.org/IETF-Standards-Process.html.

319. Center for Democracy & Technology, The Internet Engineering Task Force, http://www.cdt.org/standards/ietf.shtml. There are three general IETF meetings each year, designed to reinvigorate the working groups, enable them to mix and meet each other, and ensure that work is accomplished. *Id.*

320. *Id.*

321. *Id.*; Andrew L. Russell, *'Rough Consensus and Running Code' and the Internet-OSI Standards War*, 28 IEEE ANNALS HIST. COMPUTING 48 (2006) (quoting David Clark as describing the IETF philosophy as follows: "We reject kings, presidents, and voting. We believe in rough consensus and running code."); ERIC S. RAYMOND, THE ART OF UNIX PROGRAMMING ch. 17 (2003), *available at* http://www.catb.org/~esr/writings/taoup/html/ietf_process.html.

322. Center for Democracy & Technology, *supra* note 319; RAYMOND, *supra* note 321, at ch. 17.

that rough consensus has been achieved, they will enable the draft to become a Request for Comment (RFC).[323] Drafts that do not advance to the RFC stage are deleted after six months.[324] RFCs, in turn, are corrected by authors and other members of the community through field experience, and the RFC editor ultimately marks those that do not survive field testing as "not recommended" or "superseded."[325] Successful RFCs are those that are "stable, peer reviewed, and have attracted significant interest from the Internet community" and preferably have been proven through implementation experience.[326] The IETF steering committee designates successful RFCs as "proposed standards," and these may be elevated to "draft standard" status.[327] Draft standards that enjoy widespread implementation and general acceptance become Internet standards.[328] In 2003, there were 3000 RFCs and only sixty Internet standards.[329]

The IETF process, therefore, is designed to "engage and empower the broader community" rather than to authorize a single committee to develop guidelines.[330] It also emphasizes the importance of demonstrating standards with working implementations because flaws are far less likely to be detected without the reality check of field testing.[331]

The EHR systems community could develop CPGs in a similar fashion. AMIA or some other professional organization, with support from the Health Information Technology Research Center,[332] could serve the function of the IETF, coordinating working groups and shepherding the CPG development process. Anyone with credible credentials should be able to submit a draft CPG concerning EHR use, which would be distributed to the appropriate working group.[333] Drafts would be posted for public comment and move through several levels of review before being elevated to final

323. *Id.*

324. *Id.*

325. RAYMOND, *supra* note 321, at ch. 17.

326. *Id.*

327. *Id.* (explaining that this change occurs if there are "at least two working, complete, independently originated, and interoperable implementations of a Proposed Standard.").

328. *Id.*; *see also* Internet Engineering Task Force, The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force § 8.4, http://www.ietf.org/tao.html. (last visited Oct. 6, 2009) (describing the process by which standards are created).

329. RAYMOND, *supra* note 321, at ch. 17.

330. Russell, *supra* note 321, at 52.

331. *Id.* at 55 (discussing the importance of "running code" and explaining that it means that "multiple actual and interoperable implementations of a proposed standard must exist and be demonstrated before the proposal can be advanced along the standards track").

332. *See supra* note 280 and accompanying text.

333. Internet Engineering Task Force, *supra* note 328, at §§ 8.1–8.3 (discussing Internet drafts).

CPGs that are endorsed by the authoritative coordinating organization. The review process should require proponents to prove that the CPG was successfully implemented in the clinical setting. For example, those supporting a CPG concerning e-mail use would need to prove that their recommended e-mail handling procedure was satisfactory to a large cohort of patients and clinicians and did not result in an unacceptable number of adverse events. This relatively elaborate development method, however, could only succeed if a standardized EHR user interface existed[334] so that different CPGs would not need to be developed for each separate EHR product. A similar process could be used to establish user interface design guidelines as well as to refine CPGs in light of later experience with them or to modify them in response to technological innovations.

The key differences between the proposed approach and current CPG formulation are the existence of a central CPG coordinating organization, a uniform process for their approval, and an emphasis on field evaluation. Coordination by a single professional organization and approval through a careful, multi-step process, including field testing, would ensure that only the best proposed guidelines become final CPGs. It would prevent EHR system users from being flooded with CPGs that are contradictory, of varying quality, and unreliable. CPGs that are ultimately endorsed should not be met with resistance from the medical and EHR communities because the CPG development process would be inclusive and open to any qualified professional who wishes to propose a CPG or provide public comments. Furthermore, since CPGs would address use practices and not the approval, marketing, or certification of EHR systems, parties with competing financial interests should be able to cooperate in developing CPGs. If a process similar to that of the IETF were established for CPG development, it would be reasonable for courts to allow proof of compliance with final CPGs to establish a rebuttable presumption that the defendant met the standard of care in a medical malpractice case.

3. Audit Trails, User Problem Reports, and the Collection of Data about EHR System Use

The actual EHR systems and reports of user problems should yield significant information about how clinicians typically use the technology.[335]

334. *See supra* note 258 and accompanying text.

335. *See* Hoffman & Podgurski, *supra* note 13, at 154–55 (discussing audit trails and capture/replay capabilities); *supra* notes 263–66 and accompanying text (discussing regulatory requirements for adverse event reporting).

This data will be invaluable for both establishing the standard of care in litigation and developing CPGs.

EHR systems should feature audit trails, which are "generalized recording[s] of 'who did what to whom, when, and in what sequence,' " used to "satisfy system integrity, recoverability, auditing, and security requirements."[336] Effective audit trails would detail all interactions between systems and their users and between different systems. They would be similar in principle to flight data recorders that the Federal Aviation Administration requires for many airplanes.[337] Audit trails are intended to promote system validation and problem diagnosis and resolution. Consequently, these trails should include all system input and output that could affect clinical actions or could reflect the reliability, safety, usability, and security of the system. Audit trails, therefore, would enable litigants and researchers to collect significant information about how EHR systems are operating and being used.[338]

Litigants and courts would need to recognize the limitations of audit trails. These tools provide a one-dimensional view of complex and multi-dimensional processes.[339] They do not capture verbal communication between clinicians and patients, gestures, hand-written notes or instructions given to patients, or other human interactions. Nevertheless, audit trails would provide an unprecedented amount of information about patients' treatment histories.

Federal regulations requiring vendors to submit reports of significant user problems and mandating that summary reports be publicly available would also be useful for establishing the standard of care in medical malpractice cases.[340] Careful analysis of adverse event reports may reveal usability problems or common misunderstandings of a system's interface or displays. Such evidence may assist defendants in proving that a reasonable clinician would not have acted differently same in the circumstances.

---

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

337. 14 C.F.R. § 121.343 (2008).

338. *See* McLean, *supra* note 119, at 77–81 (discussing the use of EHR metadata in medical malpractice litigation).

339. *See* Jorge Aranda & Gina Venolia, *The Secret Life of Bugs: Going Past the Errors and Omissions in Software Repositories*, PROC. OF THE 2009 IEEE 31ST INT'L CONF. ON SOFTWARE ENG'G 307 (2009), *available at* http://portal.acm.org/citation.cfm?id=1555001.1555045&coll=&dl=GUIDE&type=series&idx=SERIES402&part=series&WantType=Proceedings&title=ICSE# ("The histories of even simple bugs are strongly dependent on social, organizational, and technical knowledge that cannot be solely extracted through the automated analysis of software repositories.").

340. *See supra* notes 263–66 and accompanying text (discussing regulatory requirements for adverse event reporting).

Collecting audit trail and adverse event data would be consistent with calls for a change in the way the standard of care is determined for litigation purposes. Some commentators have suggested that the standard of care should be empiricized and ascertained through physician surveys or epidemiologic studies of physician practices.[341] In the words of one author who is a judge, "statistical approaches provide a useful objective check, or yardstick, to use in judging the more subjective opinion evidence introduced by the parties."[342]

Audit trails will constitute a valuable tool for obtaining clear and unbiased evidence concerning commonly used medical practices. Empirical methods for obtaining proof of the standard of care are traditionally cumbersome and may lead to inconclusive results. Ordinarily, records must be pulled, organized, and abstracted by highly trained and highly paid specialists.[343] Some database evidence may also be criticized as representing a patient population that is too small to be statistically meaningful or including too few cases that are factually equivalent to the plaintiff's.[344] By contrast, interoperable EHR systems with audit trails would allow appropriately authorized personnel[345] to access large volumes of data and analyze it through carefully constructed electronic searches. Experts would then base their testimony on abundant records and be able to verify similarity of circumstances through well-crafted queries.

In addition, audit trails and user problem reports could supply information that would be used to formulate CPGs concerning EHR system operation. Researchers who obtain institutional review board approval and informed consent from EHR system users[346] could search audit trails to determine how clinicians are operating EHR systems and which practices

341. William Meadow, *Operationalizing the Standard of Medical Care: Uses and Limitations of Epidemiology to Guide Expert Testimony in Medical Negligence Allegations*, 37 WAKE FOREST L. REV. 675 (2002) (discussing the adoption of a data-based standard of care and explaining that the consequence of doing so "would be to shift the locus of power away from what might be considered an adversarial formulation of standard medical care towards a more rational, scientific view"); Cramm et al., *supra* note 74, at 726 (recommending the employment of physician surveys to determine customary care); Dann, *supra* note 311, at 950–51 (arguing that empirical proof sources will be helpful for jurors).

342. Dann, *supra* note 311, at 951.

343. Mello, *supra* note 295, at 849.

344. *Id.* at 848–49.

345. *See* FED. R. CIV. P. 34(c), 45(a)(1)(C) (establishing that nonparties can be compelled to produce electronic documents through a subpoena).

346. Mello, *supra* note 285, at 849. For a discussion of institutional review boards and informed consent, see Sharona Hoffman, *Regulating Clinical Research: Informed Consent, Privacy, and IRBs*, 31 CAP. UNIV. L. REV. 71, 76–80 (2003).

should be recommended. Summary reports of user problems that are posted on an HHS website would reveal similarly useful information. Thus, CPGs could incorporate the actual experience of large numbers of health care professionals to ensure that the guidelines are clinically relevant and represent best practices that a reasonable clinician could be expected to employ.

The data captured in audit trails and user problem reports could, therefore, influence and bolster expert testimony in two ways.[347] First, the reports would provide independent evidence of the standard of care by showing how practicing clinicians are operating EHR systems. Second, the information could and should be used to develop CPGs, which could in turn be introduced as evidence of professional custom. CPGs would thus be based on practices that are in reality commonly used by health care providers. There is no better proof of professional custom than actual records of what is being done in the field.

The medical profession should not allow the standard of care for EHR system use to be set through isolated medical malpractice decisions that are rarely published and emerge only after years of litigation.[348] Too much is at stake for patients and clinicians. Instead, modern technology could allow the standard of care to be elucidated in a more expedited fashion. Researchers and experts submitting proposed CPGs or CPG revisions would rely on audit trails and user problem reports to facilitate field evaluation. Furthermore, electronic communication will allow swift distribution of final guidelines to every practitioner in the country.

V. CONCLUSION

The highly-touted technology of EHR systems raises serious liability concerns for health care providers at the same time that it excites hope of dramatic improvements in health care outcomes. This Article intends to alert clinicians to the hazards of EHR system use, which cannot be ignored.

Nevertheless, several strategies and techniques can improve both the technology and the practices of those who use EHR systems and thereby diminish the risks of liability. For example, an informed consent process could educate patients about the risks of e-mail, including privacy concerns

347. Mello, *supra* note 285, at 852–53 (asserting that expert testimony would remain indispensable if empirical evidence was used in medical malpractice litigation).

348. *See generally* Peter Siegelman & John J. Donohue III, *Studying the Iceberg from Its Tip: A Comparison of Published and Unpublished Employment Discrimination Cases*, 24 LAW & SOC'Y REV. 1133, 1145–47 (1990) (discussing the process that generates published opinions).

and potential response delays.[349] Likewise, providers utilizing PHRs could ask patients to sign notifications regarding what information will be included in the PHR and to what extent clinicians will review patient input into PHRs.[350] E-mails should be screened by triage nurses, and patients should be advised never to use e-mail for urgent matters such as chest pain.[351] To address concerns about the review of voluminous EHRs in interoperable networks,[352] physicians could assign nurses to read through the records and provide them with summary reports of the patient's medical history, though admittedly, the nurses themselves might miss critical details. In the future, technology may facilitate document summarization, thus alleviating some of the concern about information overload.[353] Technology could also improve screen displays and the effectiveness of drug alerts,[354] and mandatory adverse event reporting could provide invaluable and occasionally life-saving information to purchasers and users of EHR systems.[355] Even the potential feelings of alienation experienced by patients whose doctors lavish attention on computers rather than on them[356] could be partially obviated by strategic choices. For example, doctors could strategically place computers in examination rooms to allow patients to view the screen. This would also allow them to discuss their computer activities so that patients feel that electronic chart review and other EHR work includes them and enhances their care.

The first step to improving EHR systems and reducing clinicians' risk of liability exposure is federal regulation that establishes approval and monitoring processes and EHR system standards and implementation specifications.[357] Federal regulation is essential to ensuring the safety and

349. Bovi, *supra* note 315, at W46; Alissa R. Spielberg, *On Call and Online: Sociohistorical, Legal, and Ethical Implications of E-mail for the Patient-Physician Relationship*, 280 JAMA 1353, 1356–57 (1998).

350. *See supra* note 172 and accompanying text.

351. Spielberg, *supra* note 349, at 1356–57.

352. *See supra* notes 108–11 and accompanying text.

353. Stergos Afantenos et al., *Summarization from medical documents: a survey*, 33 ARTIFICIAL INTELLIGENCE IN MED. 157, 161–73 (2005) (discussing summarization techniques and the challenges that must be overcome); Karen Sparck Jones, *Automatic summarizing: The state of the art*, 43 INFO. PROCESSING AND MGMT. 1449, 1454–58, 1476 (2007) (discussing advances in automatic summarization and its current limitations); Michael Stacey & Carolyn McGregor, *Temporal abstraction in intelligent clinical data analysis: A survey*, 39 ARTIFICIAL INTELLIGENCE IN MED. 1, 18–20 (2007) (analyzing the limitations of temporal abstractions and how it could be improved in the future).

354. *See supra* notes 145–50 and accompanying text.

355. *See supra* notes 263–65 and accompanying text.

356. *See supra* notes 101–06 and accompanying text.

357. *See supra* Section IV.A.1.

integrity of EHR systems, and health care providers should enthusiastically support such regulation. In addition, state regulation should obligate clinicians to undergo EHR system training as part of their CME requirements for license re-registration.

Regulation should be supplemented by agency guidance and CPGs,[358] which will serve the dual role of educating clinicians about proper EHR system use and elucidating the standard of care for litigation purposes. The opportunity to develop authoritative and efficacious guidance is especially ripe given that EHR systems are still in the early stages of development. Thus far, there has been no proliferation of competing CPGs generated by groups with conflicting agendas and varying levels of expertise, and CPGs that are developed responsibly could help optimize the safety and usefulness of EHR systems.[359] To that end, this Article has proposed that a central professional organization coordinate a uniform, multi-step CPG development process.[360] In addition, adverse event reports and the technology built into the systems—audit trails and electronic search features—could provide copious evidence of best practices and could also facilitate CPG formulation.[361] Reliable CPGs and published empirical evidence garnered from EHR systems could elucidate the standard of care for various aspects of EHR system use, providing instruction for clinicians and some degree of predictability in litigation.

EHR systems cannot remain unregulated and largely unscrutinized. Only with appropriate interventions will they become a blessing rather than a curse for health care professionals and patients.

358. *See supra* Sections III.A.2 & IV.B.2.
359. *See supra* Section IV.B.2.c).
360. *See supra* Section IV.B.2.d).
361. *See supra* Section IV.B.3.