TO HIPAA, A SON: ASSESSING THE TECHNICAL, CONCEPTUAL, AND LEGAL FRAMEWORKS FOR PATIENT SAFETY INFORMATION*

NICOLAS P. TERRY**

** Chester A. Myers Professor of Law, Co-Director, Center for Health Law Studies, Professor of Health Management & Policy, Saint Louis University, email: terry@slu.edu; web: http://law.slu.edu/nicolasterry. I thank my SLU research assistants, Brian Bohnenkamp and Michael Henderson, for their research and editorial help and Tracy Gunter for her valuable comments on an earlier draft.

I. INTRODUCTION

Positive regulation of the healthcare industry is quite rare; most safety (e.g., FDA) or healthcare financing (e.g., fraud and abuse) regulations being introduced are to correct abusive aspects of an otherwise functioning market. One of the few exceptions was HIPAA's "Administrative Simplification,"[1] mandating transactional standards for healthcare electronic exchanges. The HIPAA adventure has been as expensive as its returns have been disappointing.[2] Yet the Bush Administration's current healthcare information technology ("HIT") patient safety initiative is closely related technologically to HIPAA, albeit considerably more complex. While committed to solving the nation's medical error, quality, and cost problems, the Bush Administration is philosophically opposed to introducing any "son of HIPAA" regulation and certainly not disposed to financing the entire patient safety information endeavor.

In his 2005 State of the Union Address, President Bush urged Congress "to move forward on a comprehensive health care agenda with . . . improved information technology to prevent medical errors and needless costs . . . and medical liabilities reform that will reduce health care costs, and make sure patients have the doctors and care they need."[3] Behind those few words lies a health quality system in crisis. Traditional health quality regulatory schemes (including medical malpractice) have reached the limits of their perceived effectiveness. Yet, solving cost and quality issues with healthcare information technologies remains as controversial as it is expensive.

It is now six years since the initial Institute of Medicine ("IOM") report on medical error[4] and the development of healthcare transaction standards pursuant to HIPAA's mandate to introduce transactional standards for healthcare

---

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 261, 110 Stat. 1936, 2021 (1996).

2. *See*, *e.g.*, D'Arcy Guerin Gue with Randa Upham, *The HIPAA Prescription for Healthcare – Why Isn't It Working?*, HEALTH MGMT. TECH., Sept. 2004, at 34.

3. President George W. Bush, State of the Union Address 2005 (Feb. 2, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/02/20050202-11.html. The President's 2004 State of the Union address had contained remarkably similar language: "By computerizing health records, we can avoid dangerous medical mistakes, reduce costs, and improve care. To protect the doctor-patient relationship, and keep good doctors doing good work, we must eliminate wasteful and frivolous medical lawsuits." President George W. Bush, State of the Union Address 2004 (Jan. 20, 2004), *available at* http://www.whitehouse.gov/news/releases/2004/01/20040120-7.html. In contrast, the President's 2003 address mentioned tort law reform but not medical error. President George W. Bush, State of the Union Address 2003 (Jan 28, 2003), *available at* http://www.whitehouse.gov/news/releases/2003/01/20030128-19.html.

4. IOM, TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM (Linda T. Kohn et al. eds., 1999) [hereinafter TO ERR IS HUMAN].

electronic exchanges.[5] The first of these watershed events appeared to confirm that highlighting mistakes by individuals was counter-productive[6] and to herald a consensus around system or process reform.[7] The second promised a dramatically more efficient era of healthcare administrative simplification designed to reduce transaction costs and improve quality.

Traditional quality archetypes that process errors are inefficient and frequently ineffective. State medical boards are compromised by their limited resources and, more crucially, by their composition and practice.[8] As a quality improvement tool, medical malpractice law has been fatally compromised by insurance "crisis" cycles and the persistent battle for tort reform[9] such that William Sage describes an almost total politicization of the medical error and malpractice issues.[10] The tort reform movement and the rhetoric of frivolous lawsuits, defensive medicine, and the tenuous connection between malpractice awards and rising healthcare costs may have chilled suburban juries, but marginally effective tort reforms, such as increasingly narrowed periods of limitation and hard damage caps, adversely affect meritorious claims and, particularly in the case of damage caps,

---

5. Initial transaction standards were developed from 1998-2000. *See, e.g.*, Press Release, Department of Health & Human Services (HHS), HHS Proposes Administrative Simplification Standards for Health Care Transactions (1998), http://aspe.hhs.gov/admnsimp/nprm/press1.htm; Press Release, HHS, HHS Announces Electronic Standards to Simplify Health Care Transactions (2000), http://aspe.hhs.gov/admnsimp/final/press1.htm.

6. Lucian L. Leape, *Foreword: Preventing Medical Accidents: Is "Systems Analysis" the Answer?*, 27 AM. J.L. & MED. 145, 145-46 (2001).

7. *See generally* Lucian L. Leape, *Error in Medicine*, 272 JAMA 1851 (1994); James Reason, *Human Error: Models and Management*, 320 BMJ 768, 768-70 (2000).

8. Today, medical licensure reveals more about qualifications than quality. *See* Nicolas P. Terry, *Prescriptions sans Frontières (or How I Stopped Worrying about Viagra on the Web but Grew Concerned about the Future of Healthcare Delivery)*, 4 YALE J. HEALTH POL'Y, L. & ETHICS 183, 192 (2004). While willing to intervene in fraud, patient abuse, and provider impairment cases, state boards are too committed to "bad apple" and other outlier medical error explanations to deal with contemporary quality problems.

9. The malpractice system operates satisfactorily in average cases and likely had some positive deterrent effects in the 1970s and 1980s. However, outside of the mean, it exhibits too many false negatives (medical errors that do not receive compensation) and false positives (non-negligently caused adverse events that trigger compensation primarily because of catastrophic injuries). As a system it displays too many indeterminacies because it is state-based and because its outcomes are oversensitive to regional and local phenomena (e.g., elected judges, rural and urban vs. suburban juries).

10. William M. Sage, *Understanding the First Malpractice Crisis of the 21st Century*, *in* HEALTH LAW HANDBOOK (Alice G. Gosfield ed., 2003).

> Despite the health care system's acute need—indeed because of it—broad coalitions across the political spectrum are tempted to co-opt medicine to advance larger agendas about the effect of lawsuits on social stability and economic prosperity. . . [N]o matter which camp claims victory in the overall battle, the outcome will not remedy serious deficiencies in how American law deals with medical errors.

disproportionately disadvantage the most seriously harmed victims of error. Of course, tort "reform" does not deal with the medical error crisis; it merely increases the likelihood that the costs of error will be externalized to injured patients. Today, there are signs of backsliding from system reform to the culture of blame with Lucian L. Leape and Donald M. Berwick arguing that the latest malpractice crisis "has deflected interest of lawmakers from error prevention" to malpractice reform.[11]

The safety-related leveraging of process-supporting information technologies started modestly. Following the publication of *To Err is Human*[12] the Senate Committee on Appropriations directed the Agency for Healthcare Research and Quality ("AHRQ") to take the lead in improving patient safety.[13] In its subsequent *Crossing the Chasm* report, the IOM argued, "IT [Information Technology] has enormous potential to improve the quality of health care."[14] Today, institutional reformers inside and outside the federal government concentrate on little else. Contemporary health quality reform pays only lip service to patients and doctors. All the energies are focused on institutional reform; process reform by institutions for institutions. Federal agencies[15] and NGO's[16] are driving quality, error-reduction, and cost-savings.

This emphasis on IT does not sit well with some commentators. Bemoaning the way in which AHRQ is now concentrating its patient safety research dollars

---

11. Lucian L. Leape & Donald M. Berwick, *Five Years After To Err Is Human: What Have We Learned?*, 293 JAMA 2384, 2384 (2005).

12. IOM, *supra* note 4.

13. *See generally* AGENCY FOR HEALTH CARE RESEARCH AND QUALITY (AHRQ), AHRQ'S PATIENT SAFETY INITIATIVE: BUILDING FOUNDATIONS, REDUCING RISK, INTERIM REPORT TO THE SENATE COMMITTEE ON APPROPRIATIONS, http://www.ahrq.gov/qual/pscongrpt/ (last visited Oct. 31, 2005).

14. *See, e.g.*, IOM, CROSSING THE QUALITY CHASM: A NEW HEALTH SYSTEM FOR THE 21ST CENTURY 164, 164 (2001) [hereinafter CROSSING THE QUALITY CHASM].

15. HHS, http://www.hhs.gov/ (last visited Nov. 6, 2005); Centers for Medicare & Medicaid Services ("CMS"), http://www.cms.hhs.gov (last visited Nov. 6, 2005); Centers for Disease Control and Prevention ("CDC"), Public Health Information Network ("PHIN"), http://www.cdc.gov/phin/index.html (last visited Nov. 6, 2005); U.S. Health Resources and Services Administration ("HRSA"), http://www.hrsa.gov/ (last visited Nov. 6, 2005); U.S. Food and Drug Administration ("FDA"), http://www.fda.gov/ (last visited Nov. 6, 2005); Agency for Healthcare Research and Quality ("AHRQ"), http://www.ahrqgov/ (last visited Nov. 6, 2005); and Veterans Health Administration ("VHA"), Health Benefits & Services, http://www1.vagov/health_benefits/ (last visited Nov. 6, 2005).

16. For example, Joint Commission on Accreditation of Healthcare Organizations ("JCAHO"), http://www.jcaho.org/ (last visited Nov. 6, 2005); the National Quality Forum ("NQF"), http://www.qualityforum.org/ (last visited Nov. 6, 2005); the National Patient Safety Foundation ("NPSF"), http://www.npsf.org/ (last visited Nov. 6, 2005); the Institute for Healthcare Improvement ("IHI"), http://www.ihi.org/ihi (last visited Nov. 6, 2005); the Leapfrog Group, http://www.leapfroggroup.org/home (last visited Nov. 6, 2005); and Markle Foundation, http://www.connectingforhealth.org/ (last visited Nov. 6, 2005).

on HIT projects,[17] Leape and Berwick have noted, notwithstanding the value they place on HIT, "this reallocation revealed a serious misunderstanding of the broad array of research that will be needed to address the safety problem, and is quickly starving the new recruits who would have pursued aspects of safety other than information technology."[18] Equally, Wears and Berg remind us:

> The misleading theory about technology is that technical problems require technical solutions; i.e., a narrowly technical view of the important issues involved that leads to a focus on optimizing the technology. In contrast, a more useful approach views the clinical workplace as a complex system in which technologies, people, and organizational routines dynamically interact.[19]

Yet, the steadfast focus on institutional quality by health quality reformers is understandable. After all, in *Crossing the Chasm*, the IOM warned, "The current care systems cannot do the job. Trying harder will not work. Changing systems of care will."[20] Leape and Berwick are forced to acknowledge that prevailing medical culture remains "a daunting barrier to creating the habits and beliefs of common purpose, teamwork, and individual accountability for successful interdependence that a safe culture requires."[21] Indeed, from survey data, Audet et al. conclude that while healthcare institutions have embraced quality improvement activities, the same cannot be said for individual physicians.[22]

It is less than surprising that safety architects have turned to solutions they believe can be implemented on an abbreviated timeline, concentrated their energies at the institutional level, and subscribed to the gospel of HIT. Politicians, from the President down, have jumped on the health IT bandwagon, with one Congressman on record saying of HIT, "[t]his is as big of an issue of saving lives as the creation of antibiotics."[23] More importantly, the reform of patient safety information appears to be one of the few healthcare initiatives where a critically divided Congress can coalesce. The sharing of a stage by

---

17. *Cf.* AHRQ, AHRQ Partnerships in Implementing Patient Safety, http://www.ahrqgov/qual/pips.htm (last visited Nov. 6, 2005) (detailing recent AHRQ-funded projects). *See generally* AHRQ, *AHRQ Opens Coffers for I.T. Adoption*, *in* HEALTH DATA MANAGEMENT, Oct. 13, 2004, *available at* http://www.healthdatamanagement.com/html/news/NewsStory.cfm?DID=12043 (reporting that AHRQ has awarded $139.5 million in HIT grants and contracts).

18. Leape & Berwick, *supra* note 11, at 2385.

19. Robert L. Wears & Marc Berg, *Computer Technology and Clinical Work, Still Waiting for Godot*, 293 JAMA 1261, 1262 (2005).

20. CROSSING THE QUALITY CHASM, *supra* note 14, at 4.

21. Leape & Berwick, *supra* note 11, at 2387.

22. Anne-Marie J. Audet et al., *Measure, Learn, And Improve: Physicians' Involvement In Quality Improvement*, 24 HEALTH AFF. 843 (2005).

23. Neil Versel, *Reps. Kennedy and Murphy Admonish Health - IT Industry,* HEALTH - IT WORLD NEWS, June 9, 2005, *available at* http://www.health-itworld.com/enews/news/06_09_606.html (last visited Dec. 26, 2005).

Senators Hillary Clinton and Bill Frist to promote their *Health Technology to Enhance Quality Act of 2005*[24] did not just send a message of bipartisanship—it was also a tacit acknowledgment that it is the only healthcare reform that is going anywhere in the next few years.

Against this background, the purpose of this article is to examine the technical and legal models for what will be referred to as process-supporting health technologies;[25] technologies that support the ongoing "process" or "system" reform movement by collecting, coding, and distributing patient safety information. This article first describes the intersecting patient safety information technologies. Second, and with particular emphasis on records technology, it examines some of the possible models for patient information distribution and describes the data model issues faced by the architects of an Electronic Health Record ("EHR"). Third, there is a critical survey of the legal issues surrounding patient safety IT systems, particularly their error and privacy costs. Fourth there is an examination of barriers to successful implementation of patient safety systems and proposed solutions. Finally, the article questions whether U.S. policymakers, regulators, and patient safety system architects should shift their focus from purely technical and financial issues to take a more patient-centric approach to the system they propose.

II. PATIENT SAFETY INFORMATION TECHNOLOGIES

A. Introduction

IT-led system reform rotates around several intersecting technologies that are at different stages of maturation. These technologies are quite different from those that turned the U.S. healthcare system into the poster child of "high-tech" medicine[26]. This reputation based itself on investments in complex and costly technologies, such as imaging, that created identifiable revenue streams and, most importantly, were reimbursable. In other sectors of the economy, companies have invested heavily in information technologies and e-commerce applications

---

24. Health Technology to Enhance Quality Act of 2005, S. 1262, 109th Cong. (2005).

25. *See*, *e.g.*, Wears & Berg, *supra* note 19.

26. A point not lost on President Bush. *See* Press Release, White House, President Discusses Health Care Information Technology Benefits (2005), http://www.whitehouse.gov/news/releases/2005/01/20050127-7.html.

> Now, look, most industries in America have used information technology to make their businesses more cost-effective, more efficient and more productive, and the truth of the matter is, health care hadn't. I mean, health care has been fantastic in terms of technological change. I mean, you see these machines in these hospitals—compared to what life was like ten years ago, things have changed dramatically.

Id.

that tend to increase access, improve service, and reduce costs for consumers. However, the healthcare industry invests an average of $3,000 per worker per year in IT compared to, for example, $15,000 invested by the financial services sector.[27]

The IT "quality" (or process-supporting) solutions currently being offered to the healthcare industry, or are in development, can be grouped into three broad categories: (1) track-and-trace technologies, such as Radio Frequency Identification ("RFID"), that positively identify drugs, dosages, equipment, and patients; (2) "order entry" appliances or "decision-support" systems ("CDSS") designed to avoid medication errors stemming from, for example, prescription illegibility; and (3) electronic records systems (what are described below as Electronic Medical Records and EHR models).

B. Track-and-Trace

"Tracking" and "tracing" technologies identify drugs, dosages, equipment, biologics, patients (and their "right-site" body parts), and clinicians. Improving techniques for positively identifying patients is a broadly held goal of patient safety organizations.[28] The two principal technologies are bar codes and Radio Frequency Identification (RFID) tags. They become important "inputs" for the patient safety information domain as increasingly they are used not only to locate that to which they are attached, but also report on interactions between two or more located objects or persons.

Barcodes are so familiar because of their extensive implementation in retail environments. They identify the product they are attached to with a combination of monochromatic wide and narrow bars and spaces.[29] Scanners illuminate the bar code and read it from the light reflected back from the white areas.[30] The simplest model, and the one with which we are all familiar, is the "linear bar code" such as the Universal Product Code ("UPC") used in supermarkets.[31]

In the healthcare industry these codes are extensively implemented to code larger items and boxes of smaller ones. However, linear codes are quite large and are therefore ill suited to marking small objects such as, for example, individual medication doses.[32] Two-dimensional bar codes[33] can store more characters in

---

27. Steve Lohr, *Health Industry Under Pressure to Computerize*, N.Y. TIMES, Feb. 19, 2005, at C10.

28. *See, e.g.*, JCAHO, 2006 CRITICAL ACCESS HOSPITAL AND HOSPITAL NATIONAL PATIENT SAFETY GOALS (2005), http://www.jcaho.org/accredited+organizations/patient+safety/06_npsg/06_npsg_cah_hap.htm.

29. Press Release, Baxter International Inc., Enlightened HRBC Fact Sheet (2002), http://www.baxter.com/about_baxter/news_room/news_releases/2002/barcode_factsheet.html.

30. *Id.*

31. *Id.*

32. Baxter Int'l Inc., *supra* note 29.

33. *See generally* Bar Code 1, http://www.adams1.com/pub/russadam/stack.html (last visited

a given space and do not require the scanner to be in a direct line-of-sight.[34] They are, nevertheless, still too large for individual drug doses. As a result, the bar code industry has developed reduced space symbology ("RSS") codes[35] that, when combined with high-resolution printing techniques,[36] can be applied to very small objects. It is this technology that is at the heart of the FDA's 2004 rulemaking that requires, *inter alia*,[37] barcoding for all unit dose drugs and biologics. Currently, hospital groups are urging the FDA to extend the rule to medical devices,[38] while the Joint Commission for Accreditation of Healthcare Organizations (JCAHO) has recently articulated a safety goal to "label all medications, medication containers (e.g., syringes, medicine cups, basins), or other solutions on and off the sterile field in perioperative and other procedural settings."[39]

Notwithstanding the advances in bar code technologies and its very low per unit cost, there are inherent limitations in the technology. As a result, it is likely that much of the "tracking" and "identifying" market will shift to RFID. An RFID system consists of a reader and a tag. Typically, the RFID reader emits a radio signal, activating the transponder in the tag that is printed on, attached to, or implanted in an object or person. Once activated, the tag transponder sends data back to the reader.[40] RFID is more likely to be used to identify something specifically rather than generically.[41] For example, the UPC code contained in a bar code on a bottle of aspirin is the same for all aspirin bottles of that size made by that manufacturer. In contrast, an RFID tag placed on a particular Rx drug bottle will differentiate that specific bottle from all others.

RFID technology has several obvious advantages over bar codes: it does not require line-of-sight scanning; the code does not have to be surface-mounted; and the core technology is scaleable (and so is more likely to accommodate escalating

---

Oct. 31, 2005).

34. Elena Malykhina, *Bar Codes Expected To Have A Long Life*, INFO. WK., Oct. 21, 2004, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=51000135.

35. *See* GS1, THE GLOBAL LANGUAGE OF BUSINESS: RSS AND COMPOSITE SYMBOLOGY A NEW DEVELOPMENT IN BARCODING, http://www.gs1.org/index.php?http://www.ean-int.org/rss_intro.html&2 (last visited Oct. 31, 2005).

36. Baxter Int'l Inc., *supra* note 29.

37. *See generally* Bar Code Label Requirement for Human Drug Products and Biological Products, 69 Fed. Reg. 9120 (Feb. 26, 2004).

38. Letter from American Hospital Association and others to Lester Crawford, Acting Commissioner of Food and Drug Administration (2005), *available at* http://www.aha.org/aha/advocacy-grassroots/advocacy/agencyletters/ content/050509barcode.pdf.

39. JCAHO, *supra* note 28, at Goal 3D.

40. Jim Harper, *RFID Tags and Privacy: How Bar-Codes-On-Steroids Are Really a 98-Lb. Weakling*, 89 CEI ON POINT 2, June 21, 2004, http://www.cei.org/pdf/4080.pdf [hereinafter *RFID Tags and Privacy*].

41. *Id.* at 4.

data demands). Further, unlike read-only bar codes, RFID chips are read-write,[42] and RFID has the potential to better integrate with implantable technologies[43] such as wireless patient monitoring devices.[44]

There are two broad types of RFID technologies: active and passive. Passive RFID tags are very small and quite inexpensive,[45] with unit costs expected to fall to five cents by 2006.[46] Passive tags do not have their own power supply but derive sufficient power to respond from the magnetic fields emitted by the scanners that monitor them.[47] Typically, passive tags operate up to a distance of a few feet.[48] In contrast, active tags are larger and have their own power supplies. They are capable of emitting signals throughout a hospital floor or even an entire institution, allowing tracking of bags of contaminated waste, larger pieces of hardware, medical staff, or patients.[49] The performance of RFID systems is also a function of the radio frequency on which they operate: low frequency systems use less power, are less expensive, and penetrate objects and fluids, but have a short range; high frequency systems lack the advantages of low frequency ones but have a dramatically higher range.[50]

The core value proposition of RFID, and the one that explains its traction in the healthcare industry, is its positive impact on "supply chain efficiency," including inventory control and improved protection against drug diversion and counterfeit products.[51] RFID will be an increasingly important source of patient safety information and error reduction. For example, an adhesive tag placed near the correct site of impending surgery can be encoded on-site with the type of procedure and the surgeon's name.[52] Similarly, an RFID enabled medical implant

---

42. *See, e.g.*, James Reiner & Mike Sullivan, *RFID in Healthcare: A Panacea for the Regulations and Issues Affectiving the Industry?* (2005), http://www.ups-scs.com/solutions/white_papers/wp_RFID_in_healthcare.pdf.

43. Mark Hagland, *Bar Coding and RFID*, *in* HEALTHCARE INFORMATICS, NINE TECH TRENDS 36 (2005), http://www.healthcare-informatics.com/issues/2005/02_05/cover.htm#bar.

44. *See*, *e.g.*, Surgichip, http://www.surgichip.com/ (last visited Nov. 6, 2005); *See generally* Rob Stein, *Implantable Medical ID Approved By FDA*, WASH. POST, Oct.14, 2004, at A01.

45. Hagland, *supra* note 43.

46. *See* Reiner & Sullivan, *supra* note 42, at 1.

47. *Id.* at 3.

48. Hagland, *supra* note 43.

49. *See id.*

50. Harper, *supra* note 40, at 3.

51. *See generally* Gardiner Harris, *Tiny Antennas to Keep Tabs on U.S. Drugs*, N.Y. TIMES, Nov. 15, 2004, at A1.

52. *See* Rob Curtis, *New ID Tag Could Prevent Surgical Errors*, USA TODAY, Nov. 20, 2004, *available at* http://www.usatoday.com/tech/news/techinnovations/2004-11-20-surgichip_x.htm.

Additionally, a digital photograph of the patient and the tagging information can be integrated in the patient's EMR record. *See Patient tagging 'first in world'*, BBC NEWS, (2004), http://news.bbc.co.uk/go/pr/fr/-/1/hi/england/west_midlands/3957743.stm.

could have patient and procedure data added subsequently:[53] a test tube filled with a specimen could be written to with the patient's identification or the routing for the specimen, and RFID-equipped surgical instruments can be certified as properly cleaned after visiting an RFID-tagged sterilization chamber.[54] Once patients, drugs, and equipment are tagged, necessary equipment closest to a patient can be identified and alerts can be automated if, for example, a particular drug enters the room of a patient who is allergic to it[55] or a cadaver goes missing.[56]

In the short-term, RFID and bar code technologies likely will co-exist,[57] but as RFID costs decrease and technical issues (such as the possible interference of RF signals with devices like pacemakers) are solved, RFID will become the dominant tracking technology[58] and a significant source of patient safety data.

C. Order Entry and Decision Support

"Order Entry" and "Decision Support" technologies primarily target preventable adverse drug events; "errors in the processes of ordering, transcribing, dispensing, administering, or monitoring medications."[59] Entry technologies consist of computerized physician order entry ("CPOE") systems that seek to avoid medication errors caused by illegibility and other recording mistakes.[60] CPOEs typically are cart-mounted, tablet, or handheld PCs that avoid handwriting and transcribing errors by, for example, forcing prescribers into using pre-defined fields (such as dosage) and other standardized formats that clarify their intent.[61] Much of the impetus for CPOE adoption has come from *The*

---

53. *See e.g.*, Press Release, Zarlink Introduces World's First Wireless Chip Designed Specifically for In-Body Communications Systems (2005), http://news.zarlink.com/archive/2005/May/31/May31-ZL70100-English.htm.en.

54. *See* Reiner & Sullivan, *supra* note 42.

55. Chris Berdik, *Technology Now Used on Toll Roads and in Stores is Moving into Hospitals*, BOSTON GLOBE, Feb 1, 2005, *available at* http://www.boston.com/news/globe/health_science/articles/2005/02/01/technology_now_used_on_toll_roads_and_in_stores_is_moving_into_hospitals/.

56. Charles Ornstein & Rebecca Trounson, *Answer to Scandal: Barcodes in Cadavers*, L. A. TIMES, Jan. 20, 2005, at A1.

57. Malykhina, *supra* note 34.

58. *See generally* Hagland, *supra* note 43.

59. Rainu Kaushal & David W. Bates, *Computerized Physician Order Entry (CPOE) with Clinical Decision Support Systems (CDSSs), in* AHRQ, MAKING HEALTH CARE SAFER, A CRITICAL ANALYSIS OF PATIENT SAFETY PRACTICES 61 (Kaveh G. Shojania et al. eds, 2001), *available at* http://www.ahrq.gov/clinic/ptsafety/pdf/ptsafety.pdf.

60. *See generally* PETER KILBRIDGE WITH ASSISTANCE FROM KATY GLADYSHEVA, E-PRESCRIBING (2001), http://www.chcf.org/documents/hospitals/EPrescribing.pdf.

61. *See*, *e.g.*, Medical Communications Systems, http://www.medcomsys.com/MCS/product/pmcpoeoverview.asp (last visited Oct. 31, 2005).

Leapfrog Group, which has provided extensive guidelines for their adoption and use[62] (and inadvertently, therefore, suggested a new standard of care to malpractice lawyers), and from AHRQ, which has conducted research and provided funding.[63]

A clinical decision support system ("CDSS") is software (frequently running on or interfacing with proprietary hardware) "designed to be a direct aid to clinical decision-making, in which the characteristics of an individual patient are matched to a computerized clinical knowledge base and patient-specific assessments or recommendations are then presented to the clinician or the patient for a decision."[64] A CDSS supplements entry systems by, for example, checking for drug interactions and suggesting corollary orders.[65] When combined with additional technologies, such as "smart" drug carts,[66] these systems reduce dispensing, administering, or monitoring errors. Preliminary research suggests a decline in primary care prescription costs,[67] as well as length of stay and antibiotic costs in intensive care units.[68]

A CDSS references drug interaction information, EHR data, and potential treatment models (such as outcomes data, clinical practice guidelines, and eventually evidence-based research).[69] CDSS technologies sometimes are referred to as "surveillance" systems. While an accurate description, this seems less popular in the literature, no doubt in part because of its "big brother" connotations.

There are, of course, operational differences between the various commercial and "home-brewed" CDSS implementations; primarily differences in whether the systems "push" data (for example, alerts or clinical management plans) to the physician without being asked, or whether they only respond to requests for

---

62. Press Release, Leapfrog Group, New Guide For Hospitals On Computerized Physician Order Entry (CPOE) Gives Hospitals Much Needed Resource (2001), http://www.leapfroggroup.org/media/file/Leapfrog-FCG_Press_Release-12-06-02.pdf. *See also* JANE METZGER & FRAN TURISCO, LEAPFROG GROUP, COMPUTERIZED PHYSICIAN ORDER ENTRY: A LOOK AT THE VENDOR MARKETPLACE AND GETTING STARTED (2001), http://www.leapfroggroup.org/media/file/Leapfrog-CPO_Guide.pdf.

63. Kaushal & Bates, *supra* note 59.

64. Ida Sim et al., *Clinical Decision Support Systems for the Practice of Evidence-based Medicine*, 8 J. AM. MED. INFORMATICS ASS'N 527, 528 (2001).

65. Kaushal & Bates, *supra* note 59, at 59.

66. *See*, *e.g.*, MDG MEDICAL, REDUCING HUMAN ERROR AND ENSURING PATIENT SAFETY (2005), http://www.mdgmedical.com/ServerRx.html.

67. *See*, *e.g.*, S. Troy McMullin et al., *Impact of an Evidence-Based Computerized Decision Support System on Primary Care Prescription Costs*, 2 ANNALS FAM. MED. 494-498 (2004).

68. *See*, *e.g.*, Vitali Sintchenko et al., *Handheld Computer-based Decision Support Reduces Patient Length of Stay and Antibiotic Prescribing in Critical Care*, 12 J. AM. MED. INFORMATICS ASS'N. 398, 401 (2005).

69. *See generally* Ida Sim et al., *supra* note 64.

advice.[70] Much of the controversy over CDSS systems is rooted in the content of the knowledge base that prompts the recommendation provided to the physician. Standard drug and dosage information or even information derived from studies of patient outcomes should not be too controversial. However, the future of CDSS lies in the integration of clinical practice guidelines ("CPGs") and evidence-based medicine.[71] Yet, both CPGs and "evidence-based practice" remain controversial among many physicians.

There are increasingly positive trends showing CPOE and CDSS adoption in hospitals; trends not replicated in physician offices. A 2005 survey by Forester Research and the American Medical Association (AMA) found that only a small percentage of physicians with handheld devices use them for clinical purposes, though a far larger number use them for administrative purposes. Sixty percent of physicians in practices that have implemented electronic prescribing use their handhelds to write prescriptions and even more use the devices to check medication information.[72]

When originally introduced, CPOEs were relatively passive devices. Today, it is still possible to have CPOE technologies without a CDSS "back-end,"[73] or vice versa.[74] In practice, however, the two technologies are merging in large part because research has suggested that combined CPOE-CDSS systems offer considerable advantages over freestanding CPOE systems.[75] In the medium term, the CPOE or "front-end" will likely merge with Electronic Medical Records (EMR) entry technologies and the back-end CDSS will merge with the healthcare institution's EMR, just as such institutions will merge their EMR and imaging storage and retrieval systems.[76] Particularly once merged, the CPOE/EMR will be the dominant input for patient safety information and, as already noted, the CDSS increasingly will be the recipient of safety data generated by EHR systems.

---

70. *See generally* Charles P. Friedman et al., *Do Physicians Know When Their Diagnoses Are Correct? Implications for Decision Support and Error Reduction*, 20 J. GEN. INTERNAL MED. 334-39 (2005).

71. *See generally* Ida Sim et al., *supra* note 64.

72. Caroline Broder, *Survey: PDAs, Handhelds Under-Utilized for Clinical Applications*, HEALTHCARE IT NEWS, Mar. 23, 2005, *available at* http://www.healthcareitnews.com/NewsArticleView.aspx?ContentID=2676.

73. *See* Wikipedia, *Front-end Back-end*, http://en.wikipedia.org/wiki/Back-end (last visited Oct. 31, 2005).

74. Kaushal & Bates, *supra* note 59, at 59.

75. *See*, *e.g.*, Anne Bobb et al., *The Epidemiology of Prescribing Errors: The Potential Impact of Computerized Prescriber Order Entry*, 164 ARCH. INTERNAL MED. 785 (2004); Bernard Fernando et al., *Prescribing Safety Features of General Practice Computer Systems: Evaluation Using Simulated Test Cases*, 328 BMJ 1171 (2004).

76. *See*, *e.g.*, *Kaiser Tries to Wed One App to Many*, HEALTH DATA MGMT., June 3, 2005, http://healthdatamanagement.com/html/news/NewsStory.cfm?DID=12751.

D. Electronic Medical Records

The electronic medical (or patient) record (EMR) is hardly a new technology. Some form of electronic system is increasingly common in hospitals and doctor's offices, even if it started life as an office management, billing, or scheduling tool. Less common is a true comprehensive EMR that replaces paper within institutions. Even mature healthcare systems (in Australia, Europe, and the United States) have made only limited progress towards delivering functioning EMR systems.[77] Senator Hillary Clinton described the state of medical records keeping in the United States as "in the Dark Ages,"[78] and, unfortunately, it is still hard to disagree with the IOM's 2003 opinion:

> In most of the nation's hospitals, orders for medications, laboratory tests, and other services are still written on paper, and many hospitals lack even the capability to deliver laboratory and other results in an automated fashion. The situation is no different in most small practice settings, where there has been little if any migration to electronic records.[79]

Even a modest hospital or physician office EMR system dramatically increases the amount of patient safety information collected, with all the attendant confidentiality and security risks. It is the "record of the periodic care provided mainly by one institution."[80] Some of the largest private providers have increased the pace of EMR adoption. For example, Kaiser Permanente, the largest non-profit HMO in the United States, with more than eight million members in nine States and 12,000 doctors, has recently adopted a three-year, United States $1.8 billion EHR/EMR program[81] known as KP HealthConnect.[82] In the public

---

77. Nicolas P. Terry, *Electronic Health Records: International, Structural, and Legal Perspectives*, 12 J.L. & MED. 26, 30-36 (2004).

78. Devlin Barrett, *Clinton, Frist Tout Medical Records Bill*, NEWS & OBSERVER, June 16, 2005, *available at* http://newsobserver.com/24hour/politics/story/2485565p-10829257c.html.

79. IOM, KEY CAPABILITIES OF AN ELECTRONIC HEALTH RECORD SYSTEM 3 (2003). [hereinafter KEY CAPABILITIES OF AN ELECTRONIC HEALTH RECORD SYSTEM].

80. ROYAL COLLEGE OF GENERAL PRACTITIONERS, HEALTH INFORMATICS TASK FORCE, ELECTRONIC PATIENT RECORD STUDY, SCOPE EPR (1998), http://www.schin.ncl.ac.uk/rcgp/scopeEPR/report/i-a-22.htm.

81. Rhonda L. Rundle, *Big HMO Plans to Put Medical Records Online*, WALL ST. J., Feb. 4, 2003, at D4.

82. Debora Vrana, *Kaiser's Prescription for Medicine is Digital Hoping to Cut Costs and Improve Care, the HMO is Computerizing All of its Patient Records*, L.A. TIMES, May 30, 2005, at C1; *See also* Scott Shepard, *Baptist puts $50M in Paperless System*, MEMPHIS BUS. J., July 8, 2005, *available at* http://www.bizjournals.com/memphis/stories/2005/07/11/story1.html?GP=OTC-MJ1752087487; Nancy Ferris, *Tennessee backs BlueCross Records Project*, HEALTH IT, July 12, 2005, *available at* http://www.govhealthit.com/article89471-07-06-05-Web (describing "Community Connection," a BlueCross BlueShield project that will lead EMRs for four million Tennessee residents).

sector, the Department of Veterans Affairs ("VA") has established itself as the poster child for publicly funded and *provided* healthcare committed to process reform and technologically mediated delivery of services.[83] It has made considerable progress with its system-wide VistaEMR system.[84] Notwithstanding such efforts, EMRs are in place at only eighteen percent of hospitals, twenty-five to thirty percent of group practices, and ten percent of physician offices.[85]

In smaller practices, these low adoption rates are a function of cost. In late 2004, the average cost for an integrated records system was $7,232 per physician per year or $603 per month; considerably higher than the $100 per month target urged on the industry by the federal government.[86] The primary technical issue with EMR technology is that more than 250 software vendors currently market EMR products and none of those products allow for true data interoperability.[87] It is this lack of interoperability that is at the root of the movement towards the Electronic Health Record.

E. The Electronic Health Record

1. Introduction

An EHR, described as the "central nervous system" of the healthcare system,[88] seeks to link or otherwise leverage the patient safety information contained in existing information silos such as hospital EMRs. In the words of Joan S. Ash and David W. Bates, "[a]t its most sophisticated or most infused level, the EHR becomes a hub of all activity, something that permeates every element of the workflow and of work life."[89] Thus, broadly conceptualized, a comprehensive, longitudinal EHR will: (1) "interconnect with and enhance other error-reducing and cost-saving technologies such as decision support systems," (2) "streamline health care dataflow using an interoperable and standardized nomenclature," (3) "improve quality by encouraging accurate and legible communication among

---

83. *See*, *e.g.*, NATIONAL CENTER FOR PATIENT SAFETY (NCPS), CREATING A CULTURE OF SAFETY, http://www.patientsafety.gov/vision.html (last visited Oct. 31, 2005).

84. *See infra* text accompanying note 325.

85. Laura Landro, *The Informed Patient: Five Innovations Aid the Push To Electronic Medical Records*, WALL ST. J., Feb. 9, 2005, at D5.

86. *Survey: Records Prices Cross the Line*, HEALTH DATA MGMT. (2005), *available at* http://www.healthdatamanagement.com/html/news/NewsStory.cfm?DID=12475.

87. David C. Kibbe et al., *The Continuity of Care Record*, 70 AM. FAM. PHYSICIAN 1220, 1222 (2004) (citing unpublished CHIT data).

88. Paul M. Ellwood, *Shattuck Lecture: Outcomes Management: A Technology of Patient Experience*, 318 NEW. ENG. J. MED. 1549, 1550 (1988).

89. Joan S. Ash & David W. Bates, *Factors and Forces Affecting EHR System Adoption: Report of a 2004 ACMI Discussion*, 12 J. AM. MED. INFORMATICS ASS'N 8, 10 (2005), *available at* http://www.j-amia.org/cgi/content/full/12/1/8 [hereinafter *Factors and Forces*].

providers," (4) "automate adverse event and medical error disclosure," and (5) "facilitate reliable and reproducible outcomes research and reporting."[90]

There are several forces, error and reduction aside, relating to healthcare delivery driving the United States interest in a national EHR system.[91] These include the shift from in-patient to ambulatory care (and other episodic models) that accelerated the need for accurate and efficient flow of patient medical and billing information between organizationally and geographically distinct providers. Second, the operational aspects of managed care (such as the needs of "gate keeping" physicians who authorize referrals, demands by payers for performance "report cards," and system administrators' increasing needs for sophisticated utilization review and risk management tools) increased the need for data transparency.[92] Third, the growth of "shared care," whereby the patient shares responsibility with the provider for care and is likely to have increasingly fragmented or episodic relationships with multiple providers, requires that patients must have access to health data generally and, more controversially, information in their record.[93] Furthermore, "shared care" requires that providers have transparent access to other occasions of treatment, particularly pharmacotherapy. Finally, both patients and regulators are demanding increasing amounts of data regarding errors and outcomes in populations;[94] data that is difficult to generate without sophisticated data coding and nearly impossible to analyze without complex, comprehensive database systems.

Among United States policymakers and politicians, the adoption of a national, interoperable EHR system has become the Holy Grail of patient safety. Absent the ability of individual, siloed EMRs to transfer information between them, the current shortfall in patient safety data, including missing clinical information during patient visits,[95] will continue. Without data interoperability, our healthcare system lacks the most important source for broad scale outcomes research.

---

90. Tracy D. Gunter & Nicolas P. Terry, *The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions*, 7 J. MED. INTERNET RES. e3 (2005), http://www.jmir.org/2005/1/e3/#ref73.

91. Terry, *supra* note 77, at 28-29.

92. Paul C. Tang & W. Ed Hammond, *A Progress Report on Computer-Based Patient Records in the United States*, *in* IOM, THE COMPUTER-BASED PATIENT RECORD; AN ESSENTIAL TECHNOLOGY FOR HEALTH CARE, REVISED EDITION (Richard S. Dick et al. eds., Nat'l Head. Press 1997). http://books.nap.edu/html/computer/commentary.html. (last visited Oct. 31, 2005).

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

94. *See*, *e.g.*, Laura Landro, *The informed patient: Consumers Need Health-Care Data*. WALL ST. J., Jan. 29, 2004, at D3.

95. *See*, *e.g.*, Peter C. Smith et al., *Missing Clinical Information During Primary Care Visits*, 293 JAMA 565 (2005).

2. Policy and Process: The Decade of Health Information Technology

Moving to a national EHR[96] is not a new goal, but until quite recently, progress has been glacial.[97] The HIPAA statute re-tasked the National Committee on Vital and Health Statistics ("NCVHS"), a statutory body that advises the United States Secretary of Health and Human Services ("HHS"),[98] to become the primary advisory group for health information policy, essentially overseeing the development of the nation's health information systems.[99] The NCVHS Interim Report in June 2000 sketched a broad model for a National Health Information Infrastructure ("NHII") as the:

> set of technologies, standards, applications, systems, values, and laws that support all facets of individual health, health care, and public health. The broad goal of the NHII is to deliver information to individuals—consumers, patients, and professionals—when and where they need it, so they can use this information to make informed decisions about health and health care. . . . The content of the NHII will be varied and complex. It includes clinical, population, and personal data; practice guidelines; biomedical, health services, and other research findings; and consumer health information. . . . In effect, the content moves beyond data to information and, ultimately, to knowledge based on analysis and experience.[100]

---

96. Parallel to federal and private sector initiatives, several states have announced statewide patient information networks or EHR systems. These include Kentucky (SB 2, signed by Governor, March 2005), New Jersey (*N.J. to Create Electronic Medical Records System*, PHILADELPHIA BUS. J., May 11, 2005, *available at* http://philadelphia.bizjournals.com/philadelphia/stories/2005/05/09/daily24.html), Wisconsin (Anita Weier, *$10m for Medical Records in Budget*, CAPITAL TIMES, Feb. 4, 2005, at 3A) (reporting establishment of state Health Care Quality and Patient Safety Board to develop statewide health IT system by 2010). However, given the current perilous condition of state healthcare funding, questions remain as to how such projects will be funded. We are also seeing preliminary results from regional or local demonstration programs many of which were funded by "Connecting Communities for Better Health" under the Foundation for eHealth Initiative, http://ccbh.ehealthinitiative.org/about/default.mspx (last visited Dec. 21, 2005), that is itself partially funded by federal government grants. *See generally* Stacy Lawrence, *Regional Electronic Medical Record Efforts Get Grants*, eWEEK, July 22, 2004, http://www.eweek.com/article2/0,1759,1626136,00.asp.

97. *See generally* Eta S. Berner et al., *Will the Wave Finally Break? A Brief View of the Adoption of Electronic Medical Records in the United States*, 12 J. AM. MED. INFORMATICS ASS'N 3, 3-4 (2005), *available at* http://www.jamia.org/content/vol12/issue1/ [hereinafter *Will the Wave Finally Break?*].

98. 42 U.S.C. § 242k(k) (2000).

99. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 263, 110 Stat. 1936, 2031 (1996).

100. NAT'L COMM. ON VITAL & HEALTH STATISTICS, TOWARD A NAT'L HEALTH INFO. INFRASTRUCTURE INTERIM REPORT (2000), *available at* http://ncvhs.hhs.gov/NHII2kReport.htm.

As discussed below[101] HIPAA's EDI transactional model was the first interoperable data model to sit on this infrastructure. Although there is a general interlocking of EHR developments, the most recent foundational initiatives came from the non-governmental IOM[102] and NCVHS. It was the initial work of these two bodies that identified the technical properties of the United States patient safety data model and hinted at its architecture.[103]

Representing the private sector in the EHR movement has been the "Connecting for Health"[104] initiative funded by the Markle Foundation.[105] One of the key components of that initiative is a "Working Group on Policies for Coordination across the EHR and the PHR",[106] which is concentrating on data standards[107] with a view to "[a]ccelerating the rate of adoption of national clinical data standards in order to facilitate true interoperability".[108] Overlapping with this initiative is the work of the EHR Collaborative,[109] which consists of the major professional stakeholders such as the AMA and the Healthcare Information and Management Systems Society.[110]

Plans for a national EHR may still be somewhat aspirational, but the issue is no longer on the back burner. On April 26, 2004, President Bush announced his goal of assuring that most Americans have electronic health records within the

---

101. *See infra* text accompanying note 153.

102. The IOM is a member of the National Academies of Science, which received its charter from the United States Congress as an independent advisory body. *See* http://www.iom.edu/faq.asp?id=2959 (last visited Oct. 31, 2005).

103. NAT'L COMM. ON VITAL & HEALTH STATISTICS, REPORT TO THE SEC'Y OF THE U.S. DEPT. OF HEALTH & HUMAN SERVS. ON UNIFORM DATA STANDARDS FOR PATIENT MEDICAL RECORD INFO. (2000), http://www.ncvhs.hhs.gov/hipaa000706.pdf [hereinafter UNIFORM DATA STANDARDS]; Letter from John Lumpkin, Chair, National Committee on Vital and Health Statistics to Tommy G. Thompson, Secretary, U.S. Dept. of Health and Human Servs. (Nov. 5, 2003), *available at* http://www.ncvhs.hhs.gov/031105??3.pdf [hereinafter Letter from John Lumpkin]; KEY CAPABILITIES OF AN ELECTRONIC HEALTH RECORD SYSTEM, *supra* note 79, at n.26 and App. E, *available at* http://www.nap.edu/books/0309090776/html.

104. *See* Improving Health in the Information Age, http://www.connectingforhealth.org. (last visited Oct. 31, 2005).

105. *See* Markle Foundation, http://www.markle.org/ (last visited Oct. 31, 2005).

106. *See Working Group on Policies for Coordination Across the EHR and the PHR*, CONNECTING FOR HEALTH, http://www.connectingforhealth.org/workinggroups/pol_coordinationwg.html (last visited Oct. 31, 2005).

107. THE DATA STANDARDS WORKING GROUP, REPORT AND RECOMMENDATIONS (2003), http://www.connectingforhealth.org/resources/dswg_report_6.5.03.pdf.

108. *Id.* at 4.

109. *See* EHR Collaborative, http://www.ehrcollaborative.org (last visited Oct. 31, 2005).

110. *Id.*

next ten years.[111] To this end, the President appointed[112] Dr. David Brailer to the new post of National Health Information Technology Coordinator to guide the "nationwide implementation of interoperable health information technology."[113] This broad objective was announced by then HHS Secretary Thompson as the "Decade of Health Information Technology" to be built around "a 10-year plan to transform the delivery of health care by building a new health information infrastructure, including electronic health records and a new network to link health records nationwide."[114] The more granular goals and their attendant strategies were described at that time as:

> Goal 1 - "Inform Clinical Practice:" Bringing information tools to the point of care, especially by investing in EHR systems in physician offices and hospitals.
> Goal 2 - "Interconnect Clinicians:" Building an interoperable health information infrastructure, so that records follow the patient and clinicians have access to critical health care information when treatment decisions are being made.
> Goal 3 - "Personalize Care:" Using health information technology to give consumers more access and involvement in health decisions.
> Goal 4 - "Improve Population Health:" Expanding capacity for public health monitoring, quality of care measurement, and bringing research advances more quickly into medical practice.[115]

Initially, funding for the Office of the National Coordinator for Health Information Technology ("ONCHIT") and its demonstration projects failed to find Congressional[116] or even Administration approval.[117] In mid-2005 the Congressional appropriations committee approved $75 million for ONCHIT

---

111. *Transforming Health Care: The President's Health Information Technology Plan*, http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html (last visited Oct. 31, 2005).

112. The appointment was by Presidential decree. Under the proposed Health Technology to Enhance Quality Act of 2005, the National Coordinator position would be formally established within HHS. Health Technology to Enhance Quality Act of 2005, S. 1262, 109th Cong. § 101 (2005).

113. Exec. Order No. 13335, 69 Fed. Reg. 24,059 (Apr. 27, 2004).

114. Press Release, HHS, Thompson Launches "Decade of Health Information Technology" (July 21, 2004), http://www.hhs.gov/news/press/2004pres/20040721a.html.

115. *Id.*

116. *IT Financing: Feds Hold Back Millions on Billion Dollar Concept*, HEALTH MGMT. TECH., Jan. 2005, at 12.

117. Stacy Lawrence, *Bush Brings Back Health Care IT: The President Proposes Spending an Additional 50 Million in Support of Health Care IT in 2005*, eWEEK, Jan. 29, 2005, http://www.eweek.com/article2/0,1895.1756871.00.asp.

(plus $50 million for AHRQ),[118] but its Senate counterpart cut the ONCHIT to $45.2 million potentially jeopardizing EHR prototyping.[119]

Much of the technical standards work is now centralized in the hands of the Consolidated Health Informatics ("CHI") Initiative[120] that operates under the supervision of ONCHIT. The CHI Initiative is restricted to creating standards for the federal government (as part of the overall federal government IT initiative and, specifically, the Federal Health Architecture),[121] but coordinates its activity with the private sector through NCVHS. In June 2005 HHS set up the "American Health Information Community" ("AHIC"), an advisory body "to provide a forum for interests in and outside of the Federal government to recommend specific actions that will accelerate the widespread application of health IT."[122] The goal is to open the process up to broader public scrutiny and involve more stakeholders. AHIC is not designed to be a permanent government body but is conceived of as a transitional step towards private sector HIT governance.[123]

Keen to forge a public-private partnership on the issue, the Bush Administration recently convened a "HIT Leadership Panel" drawn from executives of large companies that purchase healthcare for their employees. This Panel identified the following key imperatives:

1. Widespread adoption of interoperable HIT should be a top priority for the U.S. health care system.
2. The federal government should use its leverage as the nation's largest health care payer and provider to drive adoption of HIT.
3. Private sector purchasers and health care organizations can and should collaborate alongside the federal government to drive adoption of HIT.[124]

---

118. *House panel passes Labor-HHS Spending Bill*, AHA NEWS (2005), *available at* http://www.ahanews.com/ahanews/jsp/display.jsp?dcrpath=AHANEWS/AHANewsNowArticle/data/ann_050609_spending&domain=AHANEWS.

119. Bob Berwin, *Senate slashes HHS Health IT Budget*, GOV'T HEALTH IT, July 18, 2005, *available at* http://www.govhealthit.com/article89584-07-15-05-Web.

120. U.S. Dept. Health & Human Servs., Office of the National Coordinator for Health Information Technology (ONCHIT), http://www.hhs.gov/healthit/chiinitiative.html (last visited Oct. 9, 2005).

121. U.S. Dept. Health & Human Servs., Federal Health Architecture, http://www.hhs.gov/fedhealtharch/ (last visited Oct. 31, 2005).

122. HHS Fact Sheet, *American Health Information Community* (2005), http://www.hhs.gov/healthit/documents/FactSheet-AHIC.pdf.

123. *Id.*

124. The Lewin Group, Inc., Health Information Technology Leadership Panel, *Final Report* (2005), http://www.os.dhhs.gov/healthit/HITFinalReport.pdf.

Since his appointment to ONCHIT, Dr. Brailer has launched an extensive and often personal lobbying effort to persuade the health industry to work together on patient safety information standards.[125] In the meantime, ONCHIT has issued requests for information ("RFIs") and requests for proposal ("RFPs") as it seeks to meet its goal of a National Health Information Network ("NHIN").

In November 2004 ONCHIT issued an RFI seeking public comment on how to achieve and sustain widespread interoperability of health information technologies and health information exchange.[126] ONCHIT published a summary of the information received in June 2005[127] and followed up with RFPs to address:

> (1) Standards ("to identify, analyze, and resolve gaps and duplications within the standards industry, and propose resolution strategies and timelines"), (2) Certification ("to develop criteria that addresses EHR functionality and will include ambulatory and inpatient features, decision support features, and performance reporting."), (3) Prototypes for a NHIN Architecture ("to develop and evaluate prototypes for an Internet-based NHIN architecture that would maximize the use of existing resources such as the Internet to achieve widespread interoperability among health care software applications, particularly EHRs"), and (4) Privacy and Security Solutions for Health Information Exchange ("to assess and develop solutions to address state and business privacy and security practices that may pose challenges to interoperable health information exchange").[128]

These are informative as to the proposed U.S. Electronic Interoperable Health Record ("EIHR") architecture and will be discussed further below.[129]

Together these technologies are the future of patient safety information in the United States. CPOEs, RFIDs, and Electronic Medical Records (EMRs) will constitute the key collectors or originators of patient safety information. Data processing that takes place in CDSS and EHR systems will directly feed back into patient care, while the outcomes research that will be enabled by EHR data will first flow into evidence-based research before closing the patient safety information "loop" by informing CDSS and EHR systems. Electronic records systems (EMRs and EHRs) are not only the most important for their potential effects on healthcare costs and quality, but also as a point of intersection for all other patient safety systems. However, they are by far the most expensive to

---

125. *See, e.g.*, Steve Lohr, *Health Industry Under Pressure to Computerize*, N.Y. TIMES, Feb. 19, 2005, at C1.

126. National Coordinator for Health Information Technology; Development and Adoption of a National Health Information Network, 69 Fed. Reg. 65599 (Nov. 15, 2004).

127. HHS, Office of the National Coordinator for Health Information Technology, *Summary of Nationwide Health Information Network (NHIN) Request for Information (RFI) Responses* (2005), http://www.os.dhhs.gov/healthit/rfisummaryreport.pdf.

128. HHS Fact Sheet, *Health Information Technology Requests for Proposals* (2005), http://www.os.dhhs.gov/healthit/documents/RFPfactsheet.pdf.

129. *See infra* text accompanying note 152 et seq.

implement, and suggest the most difficult, possibly even intractable legal and regulatory issues.

III. THE ELECTRONIC HEALTH RECORD: MODELS AND STANDARDS

A. Introduction

As should be obvious from the above, there is accelerating progress towards some form of EHR solution for the United States. As noted by Berner et al.,

> What is different now from earlier eras is that two broad policy tracks related to EHR implementation are likely to converge. One track is a well-articulated and defensible NHII initiative that proposes interoperable, ubiquitous, robust EHRs. The second track focuses on the record of underperformance of our current health care system and the need to make major improvements in health care quality and safety, access, and cost.[130]

In May 2005, Secretary Leavitt called the shift to electronic records an "economic imperative" designed to "maintain health and at the same time maintain the momentum of our economy,"[131] while Leape and Berwick recently commented, "[t]he electronic health record may be, finally, an idea whose time has come."[132]

There can be no doubt that tracking, ordering, decision support, and medical records technologies will create tremendous amounts of patient safety information. There are, however, difficult questions as to how best to harness this data. In the sections that follow, these questions are labeled as Conceptual Model, System Architecture, and Data Standards.

The proposed EIHR is being built on three sets of technologies sets. First, there are the technologies that create or collect patient safety data (such as CPOE, CDSS, track-and-trace, and EMR systems). Second, a national EHR system requires a data infrastructure that permits secure, reliable communication; the proposed national health information infrastructure ("the set of technologies, standards, applications, systems, values, and laws that support all facets of individual health, health care, and public health"[133]) will be a secure network built

---

130. Berner et al., *supra* note 97, at 6.

131. Esther Landhuis, *Health Chief: Put data online*, MERCURY NEWS, May 24, 2005, *available at* http://www.mercurynews.com/mld/mercurynews/living/health/11723708.htm.

132. Leape & Berwick, *supra* note 11, at 2388.

133. The Nat'l Health Information Infrastructure, Frequently Asked Questions About NHII, http://aspe.hhs.gov/sp/nhii/Documents/FAQ.pdf (last visited Feb. 7, 2006).

on top of the existing Internet. Third, the data collected in the various healthcare information silos must be interoperable and comparable, which requires common messaging and data standards.[134]

B. Electronic Health Records: Conceptual Models

According to the IOM, the functional model for the U.S. EHR consists of:

> (1) longitudinal collection of electronic health information for and about persons,
> (2) electronic access to person and population-level information by authorized users,
> (3) provision of knowledge and decision-support systems, and
> (4) support for efficient processes for health care delivery.[135]

At the conceptual model stage, EHR architects face several fundamental questions. First, should they create a full longitudinal record that tracks a patient's interactions with healthcare providers from cradle to grave (and beyond, as familial genomic data is increasingly referenced); or, in the alternative, should some type of excerpted or summary record be adopted? Second, assuming either a longitudinal or summary EHR is used, how does the data contained in individual provider information silos (e.g., EMRs) find its way into an EHR? Are the individual records linked in some way or are the records (or portions thereof) exported to the longitudinal (or summary) EHR? Third, there is the operational question—if individual patient information is to be exported to some type of EHR, will it be "pulled" (typically in some automated manner) or "pushed" (a semi-automated scenario that is more likely to be under the control of individual physicians or patients)?

The first question, whether to use a longitudinal or summary record, is further confused by the different types of extant non-longitudinal models. While an EMR (the record maintained by a single provider) is, by definition, an information silo, it must be recognized that not all silos are created equal. Thus, an EMR maintained by a very large, integrated provider potentially would contain data similar to that found in a longitudinal EHR.[136]

At the opposite extreme to the system-wide EMR, technologies already permit patients to maintain their own EHR. This has been described as the "Personal EHR:"[137] a subscription, web-based personal database of medical information that is collected and maintained by the patient, who then controls if and to what extent

---

134. *See*, *e.g.*, UNIFORM DATA STANDARDS, *supra* note 103, at 19.
135. IOM, PATIENT SAFETY: ACHIEVING A NEW STANDARD FOR CARE 3 n.1 (2004).
136. *See*, *e.g.*, the discussion of the Kaiser system, *supra* note 82.
137. Gunter & Terry, *supra* note 90.

it is shared with providers.[138] Recently CMS issued an RFI requesting input on how best it should make data about its Medicare beneficiaries available for incorporation into such personal EHRs.[139]

Lying somewhere between the EMR "silo" and the longitudinal EHR is the Continuity of Care Record ("CCR"). The CCR is a specification being developed by the Health Information Management and Systems Society ("HIMSS") and various professional bodies.[140] Essentially, CCR defines a common text export format ("XML"[141]) from existing proprietary EMR systems that would allow portability of summary data[142] that could be given to a patient (through a web interface or loaded on a flash drive or smart card) or transferred directly to the patient's next provider.[143] CCR architects stress that it is distinct from, but not inconsistent with longitudinal EHR models.[144]

In the words of a Journal of American Medical Association ("JAMA") editorial, "[p]atient care is a team sport, and clinicians, patients, and family should be members of the team."[145] During the transition to a fully interoperable longitudinal EHR system, record fragments carried by patients will likely be an

---

138. *E.g.*, iHealthRecord, http://www.ihealthrecord.org (last visited Oct. 31, 2005); CapMed's Personal Health Record, http://www.capmed.com/products.html (last visited Oct. 31, 2005). *See generally* Laura Landro, *High-tech Tools Help Patients Manage own Medical Records*, DESERET MORNING NEWS, Feb. 28, 2005, *available at* http://www.deseretnews.com.

139. CMS Personal Health Records RFI 01, *Request for Information Centers for Medicare & Medicaid Services' Role in Personal Health Records* (2005), http://www2.eps.gov/spg/HHS/HCFA/AGG/Reference%2DNumber%2DCMSRFIOESSAC1/Attachments.html.

140. *See* Medical Records Institute, *The Concept Paper of the CCR*, http://www.medrecinst.com/pages/about.asp?id=54 (last visited Oct. 31, 2005) [hereinafter *Concept Paper of the CCR*].

141. *See generally* W3C, Extensible Markup Language (XML), http://www.w3.org/XML (last visited Oct. 31, 2005).

142. *Concept Paper of the CCR*, *supra* note 140.

143. *See generally* Kibbe et al., *supra* note 87.

144. *Concept Paper of the CCR*, *supra* note 140.

> Although the CCR is meant to address the need for continuity of care from one provider or practitioner to any other practitioner, it is not designed to be a mini EHR. Lab and x-ray and other testing results are included only to the extent the provider completing the document finds them relevant. It does not list symptoms as its primary function. Rather it lists diagnoses and the "Reason for Referral" to the next provider or diagnostician. The "Reason for Referral" may include problems or symptoms but not in the manner in which a traditional EHR uses them as the starting point for a documentation of the SOAP-type note. Nor does it include a chronology of events, in the fashion expected in an EHR.

145. Nancy C. Elder & John Hickner, *Missing Clinical Information, The System Is Down*, 293 JAMA, 617, 619 (2005).

important part of the records system, just as "sneakernet"[146] was prior to the maturation of enterprise-wide networks.

The world's most mature summary EHR model is Australia's HealthConnect.[147] HealthConnect does not create a true longitudinal record but aggregates elements extracted from a patient's existing EMR(s).[148] The elements extracted are known as "event summaries," defined as "electronic overview of a visit to a doctor or hospital, or some other health care event [containing] only the information that is relevant to the future health and care of the consumer, rather than the comprehensive notes that a doctor may keep as a record of a consultation."[149] HealthConnect utilizes a "push" model whereby data is sent from the local EMR to a centralized HealthConnect record. This should be contrasted to the proposed U.S. EHR model that seems to adopt a "pull" model whereby the centralized EHR system (or another EMR system) initiates a data request from a provider's record. Not only is the HealthConnect "event summary" less than a complete record, but it is the patient (in consultation with the relevant physician) who controls what data is included in the summary record and who may view it.[150]

As evidenced by its RFI and RFPs, ONCHIT seems committed to an interoperable EHR, or EIHR—the "nationwide sharing of health information in patient-care and public-health settings."[151] What is notable about the U.S. EIHR project as originally conceived by IOM and NCVHS, and now by ONCHIT, is that summary or excerpted alternatives to a longitudinal model do not seem to have been considered. In part, this may be excused (or at least explained) by the highly technical path onto which the U.S. project has been directed; one of technical data standards rather than conceptual models. However, the current trajectory of this model has serious autonomy and privacy implications that are addressed later in this article.

C. Electronic Interoperable Health Record Architecture

As currently envisaged, the U.S. EIHR likely will not "exist" in any specific location. In that respect, therefore, it will not be like a hospital's EMR, a HealthConnect summary record, or even a personal EHR. The EIHR model instead contemplates data from EMRs in physician offices, hospitals, and health

---

146. Webopedia, *Sneakernet*, http://www.webopedia.com/TERM/S/sneakernet.html (last visited Oct. 31, 2005).

147. *See generally* Health Connect, A Health Information Network for All Australians, http://www.healthconnect.gov.au (last visited Oct. 31, 2005).

148. Terry, *supra* note 77, at 32-33.

149. *See* Health Connect, Event Summaries,http://www.healthconnect.gov.au/building/Event.htm (last visited Oct. 31, 2005).

150. *See* Health Connect, Privacy, http://www.healthconnect.gov.au/building/Privacy.htm (last visited Oct. 31, 2005).

151. HHS Fact Sheet, *supra* note 128, at 3.

plans being interoperable, flowing between the EMRs and continually updating each other. As one EMR technologist has described it, this will be "a system of standards rather than a standard system."[152]

The technical (if not regulatory) parallels to HIPAA are transparent. For most healthcare workers and many lawyers, "HIPAA"[153] bespeaks the regulation of healthcare privacy (actually confidentiality). In actuality, the healthcare "Administrative Simplification" provisions[154] that enabled the controversial HIPAA privacy and security regulations,[155] were primarily designed to mandate healthcare transactional standards. The patient protections were enacted because of the increased privacy costs that the transactional system engendered and to limit how providers could externalize those risks to their patients.[156] At a conceptual level, the EIHR will complete the HIPAA-EDI model (that already must contend with claims attachments involving health data) and, at the process level, will share much of the EDI's informational infrastructure.

ONCHIT's development of an EIHR model seems to have two components: (1) continued encouragement of Regional Health Information Organizations ("RHIOs");[157] and (2) development of a Nationwide Health Information Network ("NHIN").[158] As to the former, the Frist-Clinton bill likely indicates a sense of ONCHIT's thinking by proposing monies be made available to "award competitive grants to eligible entities to implement regional or local health information plans to improve healthcare quality and efficiency through the electronic exchange of health information. . ."[159] These RHIOs will operate both as demonstration projects and as foundations for the NHIN if the final architecture remains decentralized.[160]

As to the latter, ONCHIT's RFP looks to "develop and evaluate prototypes for a NHIN architecture maximizing the use of existing resources such as the Internet to achieve widespread interoperability among health care software applications, particularly EHRs."[161] No doubt the contracts awarded by

---

152. *Deploying an EMR: The battle for record access*, AMEDNEWS.COM, Mar. 7, 2005 (quoting Larry Albert of Integic).

153. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 263, 110 Stat. 1936, 2031 (1996).

154. 42 U.S.C. § 1320d (2000).

155. 45 C.F.R. §§ 160, 164 (2004).

156. *See generally* Nicolas P. Terry, *An eHealth Diptych: The Impact of Privacy Regulation on Medical Error and Malpractice Litigation*, 27 AM. J.L. & MED. 361, 363-66 (2001).

157. *See generally* HHS/ONCHIT, *Regional Health Information Organizations (RHIOs)*, http://www.hhs.gov/healthit/rhio.html. (last visited Oct. 31, 2005).

158. ONCHIT, *Developing a Prototype for a Nationwide Health Information Network Architecture*, http://www.hhs.gov/healthit/nhindemos.html (last visited Oct. 31, 2005).

159. Health Technology to Enhance Quality Act of 2005, S. 1262, 109th Cong. § 2908 (2005).

160. *See generally* Health Information Technology, *HHS Is Taking Steps to Develop a National Strategy* (2005), *available at* http://www.gao.gov/new.items/d05628.pdf.

161. Developing a Prototype for a Nationwide Health Information Network Architecture 2,

ONCHIT will begin to answer some of the second level architecture questions posed by national or regional EIHRs, such as whether interoperability will lead to the creation of a separate, warehoused EHR, or whether (as seems more likely) existing records systems will contain "pointers" enabling authorized users to pull patient data from other records systems.

D. Patient Safety Information Data Standards

Assuming there is a physical communications infrastructure and secure transport and application levels,[162] a national or regional EHR model (whether summary or longitudinal) requires two core sets of data standards. The first is for data interchange formats, the second is for encoding specific data types (or health vocabulary) used in an EHR.

The challenge differs from something like the CCR because of the sophistication and complexity of the data to be exported and the requirement that this rich data can be imported and exported by multiple systems. For example, a model like CCR merely exports a patient data summary or a discrete piece of data into a generally readable text format. In contrast, a longitudinal record requires far more robust and complex data, such as granular data as to medication and diagnosis. This data must be presented in a consistent format. Furthermore, the projected uses of the data go far further than simple text export; full interoperability requires that data contained in a patient's record interact with patient safety data elsewhere (such as drug interactions or CPG databases) and then "return" to the patient record better informed. Finally, data in individual records also must be capable of deidentified extraction for reporting purposes.

An agreed set of data interchange standards provide a sophisticated electronic "envelope" for the data to be exchanged. In this regard, an EHR system requires, like HIPAA's transactional model, an Electronic Data Interchange ("EDI") standard. The agreed standard is responsible for determining "which pieces of information are mandatory for a particular document, which pieces are optional and give the rules for the structure of the document."[163] Some of the identifier and messaging standards[164] adopted by the federal government, pursuant to HIPAA of 1996,[165] to create our national healthcare transactional system (an

---

http://fs2.eps.gov/EPSData/HHS/Synopses/4607/Reference-Number-ONCHIT-3/ONCHITFinalRFP-NationwidePrototype1.pdf (last visited Oct. 31, 2005).

162. *See, e.g.*, Wikipedia, *Internet Protocol Suite*, http://en.wikipedia.org/wiki/Internet_protocol_suite (last visited Oct. 31, 2005).

163. Wikipedia, *Electronic Data Interchange*, http://en.wikipedia.org/wiki/Electronic_Data_Interchange (last visited Oct. 31, 2005).

164. *See generally* HHS, *Administrative Simplification in the Health Care Industry*, http://aspe.hhs.gov/admnsimp/index.shtml (last visited Nov. 6, 2005). An example would be standards developed by ASC X12, http://www.x12.org (last visited Oct. 31, 2005).

165. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 263, 110 Stat. 1936, 2031. HIPAA-EDI transactions, such as health plan enrollment, eligibility, payment

electronic data interchange or EDI system) are transferable to an EHR system. In the interim, these messaging formats for clinical data (as they will be used in EHRs) have been further developed by organizations such as Health Level 7 ("HL7"),[166] Digital Imaging and Communications in Medicine ("DICOM"),[167] and the National Council for Prescription Drug Programs.[168] The EHR standard for administrative data (for example healthcare transactions, billing and insurance information) is ASC X12[169] as used for the HIPAA EDI. The data exchange (or messaging) standard for clinical data is HL7.[170]

The more difficult (and patient safety information specific) challenge is to specify the standards required for EHR data to achieve what NCVHS refers to as semantic interoperability and comparability, such that "the meaning of data is consistent when shared among different parties."[171] Here, both NCVHS[172] and IOM[173] have recommended the adoption of core terminologies dealing with, for example, disease (ICD-9-CM[174]), medical procedures and services (CPT-4[175]), and drug names or doses (e.g., RxNorm[176]). Considerable development is also underway to standardize event taxonomy (such as adverse event or near-miss reporting)[177] and to capture knowledge representation (such as clinical practice guidelines). Consistent with this approach, the CHI Initiative has identified the necessary data and messaging domains and is in the process of adopting or

---

and remittance advice, claims, health plan premium payments, health claim status, and referral certification and authorization are dependent on messaging formats, transaction codes, and data element codes that are conceptually related to those being developed for EHR systems.

166. *See generally* Robert H. Dolin et al., *The HL7 Clinical Document Architecture*, 8 J. AM. MED. INFORMATICS ASS'N 552, 552–569 (2001).

167. Digital Imaging and Communications in Medicine, http://medical.nema.org (last visited Oct. 31, 2005).

168. The National Council for Prescription Drug Programs, http://www.ncpdp.org (last visited Oct. 31, 2005).

169. *See* The Accredited Standards Committee (ASC X12), http://www.x12.org (last visited Nov. 5, 2005). Specifically, *see* The X12N Insurance subcommittee, http://www.x12.org/x12org/subcommittees/sc_home.cfm?strSC=N&CFID=640006&CFTOKEN=37253298 (last visited Oct. 31, 2005).

170. *See* Health Level Seven, http://www.hl7.org (last visited Oct. 31, 2005).

171. UNIFORM DATA STANDARDS, *supra* note 103, at 6.

172. Letter from John Lumpkin, *supra* note 103.

173. KEY CAPABILITIES OF AN ELECTRONIC HEALTH RECORD SYSTEM, *supra* note 79.

174. Centers for Disease Control and Prevention, Nat'l Ctr for Health Statistics, *Classification of Diseases and Functioning & Disability*, http://www.cdc.gov/nchs/about/otheract/icd9/abticd9.htm (last visited Oct. 31, 2005).

175. American Medical Ass'n, *CPT Process –How a Code Becomes a Code*, http://www.ama-assn.org/ama/pub/category/3882.html (last visited Nov. 6, 2006).

176. Nat'l Library Medicine, *RxNorm*, http://www.nlm.nih.gov/research/umls/rxnorm_main.html (last visited Oct. 31, 2005).

177. For example, by using SNOMED CT. *See* http://www.snomed.org/snomedct/index.html (last visited Oct. 31, 2005); *see* IOM, *supra* note 135, at 26.

developing the technical standards necessary for their exchange (interoperability and comparability).[178]

IV. THE LEGAL FRAME FOR PATIENT SAFETY DATA

A. Introduction

The legal system has failed to articulate clear incentives for HIT adoption, with healthcare institutions being caught in a trap of facing liability for failing to implement emerging process-supporting technologies, but equally facing liability for implementing immature systems.[179] Additionally, emerging technologies likely will increase provider litigation risks by providing plaintiffs with secure, unalterable records that better identify all professional-patient contacts, potentially increasing the defendant pool, while identifying similarly situated patient-plaintiffs.[180] There are additional legal risks associated with financial models designed to address the market failures associated with HIT adoption.[181] Assume, for example, that a hospital supplies equipment or financial support to a doctor to enable access to its EMR. Such an arrangement could contravene the *Physician Self-Referral Act*,[182] which prohibits a physician with a financial relationship with a healthcare entity from making certain referrals to that entity. The "Stark II" regulations contain only a very limited exception in the case of "Community-wide health information systems."[183] Similarly, criminal penalties could be implicated because of the *Anti-Kickback Statute*.[184]

This section of the article explores two aspects of process-supporting technologies that have critical legal implications, yet which have received insufficient attention amid the political and industry enthusiasm for the new technologies. Those two aspects are (1) negative externalities relating to privacy, and (2) negative externalities relating to error.

In fairness, it must be acknowledged that EIHR-related discussion of autonomy or privacy may have been minimal because development has operated

---

178. For a detailed listing of domains and the adoption of standards for each, *see* HHS, *Standards Adoption Recommendation*, http://www.hhs.gov/healthit/documents/chiinitiative/CHIExecSummaries.pdf (last visited Oct. 31, 2005).

179. *See generally* Nicolas P. Terry, *When the "Machine That Goes 'Ping'" Causes Harm: Default Torts Rules and Technologically-Mediated Health Care Injuries*, 46 ST. LOUIS U.L.J. 37 (2002).

180. Terry, *supra* note 156, at 410-13.

181. *See infra* text accompanying note 278, et seq.

182. 42 U.S.C. § 1395nn (2000).

183. Exceptions to the Referral Prohibition Related to Compensation Arrangement, 69 Fed Reg. 16138, 16142 (Mar. 26, 2004).

184. 42 U.S.C. § 1320a-7b(b).

in an almost exclusively technical domain. As the difficult questions of implementation draw closer, the necessity for the involvement of all stakeholders and sensitivity to issues that are not purely technical becomes more of an imperative. There are signs that this is beginning to occur. For example, in a 2004 interview with the British Medical Journal, Dr. Brailer adopted patient-centric language: "We expect to have a network that securely and in a patient-controlled manner connects all those electronic health records . . . so that if a physician is seeing a patient all that patient's information that the patient wants the doctor to see is made available to them in real time."[185] Similarly, the proposed *Health Technology to Enhance Quality Act of 2005*[186] is far more tuned to privacy concerns and stakeholders, and the AHIC's first listed goal relates to protecting privacy as well as security.[187]

B. Privacy and Autonomy Externalities

1. In General

As HIT finds traction, we should find comfort in robust health privacy; a social good that is protected by the powerful triumvirate of ethical constraints, effective laws, and operational necessities. The reality is quite different. State and federal privacy law may be omnipresent, the pages of medical journals and law reviews may be filled with exhortations of confidentiality, and voyeurism-enabling media may be quick to pounce on system failures, but health information privacy is surprisingly fragile. The best evidence of its perilous condition is that the issue has become politicized. Take, for example, then HHS Secretary Thompson's 2001 characterization of the Administration's approach to HIPAA health privacy, "President Bush wants strong patient privacy protections put in place now," and to the federal standards intent to give "patients peace of mind in knowing that their medical records are indeed confidential and their privacy is not vulnerable to intrusion."[188]

Contrast that comforting proclamation with the actions and words of the same Administration's Department of Justice ("DOJ") in 2004. Seeking the medical records of some forty-five patients of a physician who was challenging the validity of the Partial-Birth Abortion Ban Act of 2003,[189] the DOJ argued before the federal courts that federal law "does not recognize a physician-patient. .

---

185. Anne Harding, *Interview with Nat'l Health Info. Tech. Coordinator David Brailer, MD, PhD*, 4 BMJ 328, 328 (2004).

186. Health Technology to Enhance Quality Act of 2005, S. 1262, 109th Cong. (2005).

187. HHS Fact Sheet, *supra* note 122.

188. HHS, *Statement by HHS Sec'y Tommy G. Thompson Regarding the Patient Privacy Rule* (2001), http://aspe.hhs.gov/admnsimp/final/press4.htm.

189. 18 U.S.C. § 1531 (2005).

.privilege"[190] and that patients "no longer possess a reasonable expectation that their histories will remain completely confidential."[191] While Scott McNealy's infamous remark, "You have zero privacy anyway. Get over it,"[192] is not generally true of health information, such protection is perhaps more fragile than generally thought in a post-HIPAA world.

2. Electronic Health Records

A fully longitudinal, interoperable records model fits the "perfect storm" profile of privacy advocates. The privacy externalities of medical data have been limited because of the inefficient data silos being used. Risks have been further reduced by the general lack of portability of paper records and the inexpensive security regimens (such as locked file cabinets) that apply to paper. In contrast, an EIHR model is premised on the aggregation of these silos, common data standards, and (to improve usability and maximize the return on EMR/EHR investments) the increased sophistication of data mining tools. Making patient safety information available to all healthcare providers, that are even tangentially involved in a patient's care, renders the level of privacy and security accorded that data a function of the weakest link in the system. Fully interoperable data is also immeasurably more valuable for secondary uses (e.g., marketing) and is an irresistibly tempting target for commercial aggregators.[193]

Even a cursory look at newspaper stories from around the country suggests that, in spite of HIPAA protections, our privacy and security systems remain quite dysfunctional. For example, reports during 2005 include stolen laptop computers containing medical data,[194] the theft of a computer disk containing medical and

190. This is a correct if surprising statement of the law. *See* Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923, 926 (7th Cir. 2004).

191. Robert Pear & Eric Lichtblau, *Administration Sets Forth A Limited View on Privacy*, N.Y. TIMES, Mar. 6, 2004, at A8 (quoting the Justice Dept.). The issue was raised in several district court cases, Planned Parenthood Fed'n of Am., Inc. v. Ashcroft, No. C 03-4872 PJH, 2004 U.S. Dist. LEXIS 3383 (N.D. Cal. Mar. 5, 2004); Nat'l Abortion Fed'n v. Ashcroft, No. 03 Civ. 8695, 2004 U.S. Dist. LEXIS 4530 (S.D. N.Y. Mar. 18, 2004); Citizens for Health v. Thompson, No. 03-2267, 2004 U.S. Dist. LEXIS 5745 (E.D. Pa. Apr. 2, 2004), prior to the Seventh Circuit's opinion in Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923, 926 (7th Cir. 2004) (quashing government's subpoena). Thereafter the administration withdrew its request for the documents. Terry Freiden, *U.S. Drops Fight to Get Abortion Records*, CNN (2004), http://www.cnn.com/2004/LAW/04/27/abortion.records.

192. Drew Clark, *Sun's Privacy Officer Works to Enhance Firm's Security*, NAT'L J. TECH. DAILY, Nov. 14, 2003 (comment attributed to Scott McNealy, Chairman and CEO, Sun Microsystems in 1999).

193. *See generally* Andrew Ross Sorkin & Steve Lohr, *VNU Is Nearing Deal to Buy IMS Health for $6.7 Billion*, N.Y. TIMES, July 11, 2005, at A15 (reporting acquisition of IMS Health by Dutch market research company VNU, to gain access to U.S. pharmaceutical business research).

194. Gary Delsohn, *Laptop Stolen; State Fears ID Theft*, SACRAMENTO BEE, May 28, 2005, at A3,

financial information relating to 200,000 patients,[195] the hacking of HIT systems,[196] a disgruntled ex-employee of a managed care corporation linking her blog to the medical information of 140 patients,[197] the theft of computer backups containing the personal information of 57,000 Blue Cross Blue Shield customers,[198] and Cleveland Clinic executives and security guards running through the streets to retrieve 3,000 patient records that fell from a truck and blew away.[199] Ominously, a Wall Street Journal article in 2005 reported that identity thieves regularly target hospital and nursing home patients because of the relative exposure of their social security numbers and other key identifiers while in a healthcare environment.[200]

Of course, the "answer" to health information privacy externalities should be HIPAA's privacy[201] and security[202] regulations. However, the HIPAA model is hugely flawed in concept, terminology, and implementation.[203] First and crucially, like most common law and state statutory protections that preceded the federal regulations, HIPAA does not in any way protect patient *privacy*—it merely places *confidentiality*-based limitations on information provided to healthcare entities. Worse, it expends most of its energy on the *process* of patient consent to disclosure. Second, its "more stringent" partial preemption rule guarantees a growing vector between federal and state laws.[204] Third, the HIPAA standards

---

available at http://www.sacbee.com/content/politics/story/12968265p-13815437c.html (a laptop computer stolen from a car in California contained names, Social Security numbers and personal health information for 21,600 Medi-Cal recipients).

195. *Charges in Patient Records Theft*, MERCURY NEWS, May 14, 2005, at 1B.

196. Jean P. Fisher, *Hacker Hits Duke System; Personal Data, Passwords Taken*, NEWS & OBSERVER, June 4, 2005, at D1.

197. *Kaiser adds to its lawsuit against blogger*, MERCURY NEWS, Mar. 18, 2005, at 1C. *See also* News Release, State of California, Department of Managed Health Care Orders Bay Area Blogger to Remove Kaiser Patient Information from Web (Mar. 17, 2005), *available at* http://www.dmhc.ca.gov/library/reports/ news/BApr.pdf. Subsequently, Kaiser was fined by the state Department of Managed Health Care for the security breach. *Privacy breach osts Kaiser $200,000 Fine For Leaving Patient Information On Public Web Site*, MERCURY NEWS, June 21, 2005, *available at* http://www.mercurynews.com/mld/ mercurynews/living/health/11946337.htm.

198. Matt Hanson, *Medical Firm's Files with Personal Data Stolen, Key Information on 57,000 at Risk*, ARIZ. REPUBLIC, July 13, 2005, *available at* http://www.azcentral.com/arizonarepublic/business/articles/0713biodyne13.html.

199. *Medical Records Jam Cleveland Traffic*, SCIENCE DAILY, Apr. 6, 2005, *available at* http://www.sciencedaily.com/upi/?feed=TopNews&article=UPI-1-20050406-15294000-bc-us-medrecords.xml.

200. Kevin Helliker, *A New Medical Worry: Identity Thieves Find Ways to Target Hospital Patients*, WALL ST. J., Feb. 22, 2005, at D1.

201. 45 C.F.R. § 164.500-534 (2004).

202. 45 C.F.R. § 164.302-318 (2004).

203. Nicolas P. Terry, *What's Wrong with Health Privacy?*, *in* THE LAW AND BIOETHICS (Ana Smith Iltis & Sandra H. Johnson eds., London, Routledge) (forthcoming 2006).

204. 45 C.F.R. § 160.202 (2004).

contain extremely broad carve-outs (public health, judicial, and regulatory) that do not require patient consent to data processing.[205] Fourth, the privacy standards are still too lax regarding secondary uses of patient information.[206] Fifth, there is a growing concern about the rigor demonstrated by the Office of Civil Rights in enforcing the regulations.[207]

Some more granular criticisms are particularly relevant in the context of an EIHR system. First, as is well known, when the HIPAA privacy standards were first promulgated, they required that patients be allowed to consent to disclosure for treatment, payment, or healthcare operations purposes.[208] When amended by the Bush Administration, this requirement for consent was removed[209] and replaced by the permissive statement that "[a] covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations."[210] Second, the HIPAA regulation makes no attempt to narrow the flow of patient health information to the "circle of care"—the healthcare providers *directly* involved in the patient's *current* diagnosis or treatment. Although the regulations contain a general "minimum necessary" proportionality rule,[211] it is inapplicable to "[d]isclosures to or requests by a health care provider for treatment[.]"[212]

Finally, HIPAA applies only to healthcare entities,[213] a relatively narrow purview given the range of U.S. and offshore players likely to be involved in EHR data processing. Already half of the $20 billion U.S. medical transcription industry is outsourced outside the United States.[214] and data processing involved after the launch of a complete U.S. EHR program is surely to follow. Offshore data processors of PIHI are "business associates"[215] of HIPAA "covered entities"[216] and, as such, their contractual relationships must contain certain

---

205. 45 C.F.R. § 164.512 (2004).

206. *See generally* 45 C.F.R. §§ 164.508, 164.510 (2004).

207. *See, e.g.*, Peter P. Swire, *Justice Department Opinion Undermines Protection of Medical Privacy*, CTR. AM.. PROGRESS (2005), http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=743281&printmode=1.

208. 45 C.F.R. § 164.506 (2001).

209. 45 C.F.R. § 164.506(a) (2004).

210. 45 C.F.R. § 164.506(b)(1) (2004).

211. 45 C.F.R. § 164.502(b)(1) (2004) ("When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.").

212. 45 C.F.R. § 164.502(b)(2)(i) (2004).

213. 45 C.F.R. § 160.103 (2004).

214. David Lazarus, *Looking Offshore: Outsourced UCSF Notes Highlight Privacy Risk, How One Offshore Worker Sent Tremor Through Medical System*, S.F. CHRONICLE, Mar. 28, 2004, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/03/28/MNGFS3080R264.DTL.

215. 45 C.F.R. § 160.103 (2004).

216. 45 C.F.R. § 160.103 (2004).

HIPAA limitations on data protection.[217] In an answer to an inquiry by Congressman Markey about outsourcing of sensitive data outside of the United States, then HHS Secretary Thompson admitted that his department failed to document the "nature or content" of the contracts between covered entities and their business associates, or directly regulate offshore business associates.[218] As the costs of the EIHR adventure increase (as assuredly they will), providers and data clearinghouses will be tempted to use off-shore data processing and storage. Already, we are seeing proposed federal[219] and state[220] legislation aimed at penalizing corporations that fail to disclose security breaches[221] and attempting to control "outsourcing" of sensitive data storage or processing outside of the United States.

Finally, all those involved in the development of the U.S. EIHR system must acknowledge an elephant in the room—the Department of Homeland Security and its vital and continuing fight against terrorism and (particularly in this context) bioterrorism.[222] Recently, the HHS Office of Civil Rights added the question: "Does the [HIPAA] Privacy Rule create a government database of all individuals' personal health information?" to its HIPAA privacy FAQ.[223] Its cogent and straightforward answer to the possibly paranoid questioner was: "No. The Privacy Rule does not create such a government database or require a physician or any other covered entity to send medical information to the Federal government for a government database or similar operation."[224] The difficulty, of course, is that once a national EIHR is in place, the answer to this question will, of necessity, have to be far more nuanced.

At the very least, the HIPAA regulations will require amendments to make clear that all EIHR and other health IT generated patient information is covered;

---

217. 45 C.F.R. § 164.504(e) (2004).

218. Letter from Tommy G. Thompson, Sec'y of Health & Human Services to Edward J. Markey, Congressman, U.S. House of Representatives 2 (June 14, 2004) (on file with author).

219. *See*, *e.g.*, Personal Data Offshoring Protection Act of 2004, H.R.4366, 108th Cong. (2d Sess. 2004).

220. *E.g.*, S.B. 1492 (Ca. 2004) (vetoed by Governor Schwarzenegger Sept. 2004). *See* Steve Lawrence, *Schwarzenegger Vetoes Bills to Prevent Outsourcing of Jobs*, S.F. CHRONICLE, Sept. 30, 2004, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file= /news/archive/2004/09/30/state2258EDT0266.DTL.

221. *See generally* Brian Krebs, *States Keep Watchful Eye on Personal-Data Firms*, WASH. POST, June 1, 2005, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/06/01/AR2005060100359.html.

222. *See generally* U.S. Dept. of Homeland Security, http://www.dhs.gov/dhspublic (last visited Oct. 31, 2005).

223. HHS, Questions & Answers, http://answers.hhs.gov/cgi-bin/hhs.cfg/php/enduser/std_alp.php?p_sid=xPmDQ6Gg&p_lva=&p_li=&p_page=1&p_cat_lvl1=7&p_cat_lvl2=%7Eany%7E&p_search_text=&p_new_search=1 (last visited Oct. 31, 2005).

224. *Id.*

a position taken by the proposed *Health Technology to Enhance Quality Act of 2005*.[225] In addition, the level of patient and physician trust (and, ultimately, participation) will be a function of their ability to choose the data that is included, a far tighter sense of the "circle of care," and curtailment of some of the carve-outs from the confidentiality standard.

3. Radio Frequency Identification

The privacy implications of tracking technologies are less well known. Privacy advocates, such as the Electronic Privacy Information Center ("EPIC")[226] and Consumers Against Supermarket Privacy Invasion and Numbering ("CASPIAN"),[227] are concerned that the tags will be used by enterprises for intense customer profiling both inside and outside their stores (either by not disabling the tags at checkout or by insinuating the tags into customer loyalty cards[228]). The fear is that the data will be read by third parties (from criminals to the government), removing all vestiges of privacy.[229] In contrast, those opposed to RFID-specific privacy regulation believe that technological and cost limitations will place natural impediments in the way of this Orwellian vision, while blocking technologies and existing legal schema will take care of any residual concerns.[230]

Most of the discussion has been at the level of general consumer goods rather than specifically with regard to the healthcare environment. However, EPIC has urged HHS to adopt a "Four Tier Approach" to RFID; tier 1 being the bulk distribution of products (where there is no privacy risk); tier 2 being the product distribution to the patient (where it should be considered PHI and protected by HIPAA); tier 3 being the temporary identification of patients (implicating HIPAA security and identity theft), and; tier 4 being the permanent identification of patients (with privacy implication so profound that HHS should prohibit the practice).[231]

---

225. Health Technology to Enhance Quality Act of 2005, S. 1262, 109th Cong. § 2907 (2005).

226. Electronic Privacy Info. Ctr. ("EPIC"), http://www.epic.org (last visited Oct. 31, 2005).

227. Consumers Against Supermarket Privacy Invasion & Numbering, http://www.nocards.org (last visited Oct. 31, 2005).

228. *See, e.g.*, PRADA RFID Technology, http://www.ideo.com/case_studies/prada.asp?x=2. ("An RFID tag is also part of a PRADA customer card. Customer preferences are stored on the database, and only the customer card provides access. This information is used to customize the sales experience and further enhance the service provided to the card-holding customer.") (last visited Oct. 31, 2005).

229. *See generally* EPIC, *Radio Frequency Identification (RFID) Systems,* http://www.epic.org/privacy/rfid/ (last visited Oct. 31, 2005).

230. *RFID Tags and Privacy*, *supra* note 40, at 7-12.

231. Marc Rotenberg, President, EPIC, Presentation at the Dept. of Health and Human Servs.: Privacy Implications of RFID Technology in Health Care Settings (Jan. 11, 2005), http://www.epic.org/privacy/rfid/rfid_ncvhs1_05.ppt.

The only federal agency primarily concerned with healthcare to directly address RFID implementation has been the FDA.[232] The FDA approved implantable RFID medical devices[233] and, as part of its counterfeit drugs policy, has issued a "Compliance Policy Guide" for RFID to encourage pilot projects.[234]

In most cases involving healthcare institutions, HIPAA will apply to bar code and RFID, data because those technologies fall under the definition of "identifier" of PHI.[235] Nevertheless, it has been suggested that healthcare providers using RFID technologies adopt a code of conduct.[236] Such a code would reiterate obvious provider obligations, such as notice, specific consent, and data amendment, but would also, for example, address RFID-specific issues such as the provider policy on RFID data retention and how patients can deactivate the RFID chips.[237]

RFID privacy issues will implicate a patchwork of federal and state consumer protection laws. For example, California recently reached a settlement under its unfair competition law with an automobile rental company that failed to notify its customers that it was tracking their movements using GPS devices.[238]

Some Fourth Amendment jurisprudence is also relevant. The worst fear of privacy advocates is that the federal government will make surveillance use of essentially invisible, potentially intrusive, RFID trackers. While some drug diversion cases will likely play out that way, private actors have the most to gain. Nevertheless, the Fourth Amendment cases are useful in getting a sense of judicial attitudes towards the public's expectations of privacy. The relevant line of cases dates back to *Katz v. United States*.[239] There, the Supreme Court overruled the holding in *Goldman v. United States*[240] that electronic surveillance without physical penetration of premises by a tangible object did not violate the Fourth

---

232. U.S. Food & Drug Admin., *Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs, Guidance for FDA Staff and Industry* (2004), http://www.fda.gov/oc/initiatives/counterfeit/rfid_cpg.html. Outside of the healthcare environment, the Department of Defense has announced a wide-ranging RFID policy. *See* Department of Defense, News Release No. 775-03, DoD Announces Radio Frequency Identification Policy (Oct. 23, 2003), *available at* http://www.defenselink.mil/releases/2003/nr20031023-0568.html.

233. Surgichip, *supra* note 44.

234. U.S. Food and Drug Admin., *supra* note 232.

235. "Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section. . . ." 45 C.F.R. §164.514(b)(2)(i)(R) (2004).

236. Lisa J. Sotto, *An RFID Code of Conduct*, RFID J., May 30, 2005, *available at* http://www.rfidjournal.com/article/articleview/1624/1/128.

237. *Id.*

238. News Release, Office of the Attorney General California Department of Justice, Attorney General Lockyer Announces Consumer Protection Settlement with Bay Area Rental Car Firm (Nov. 9, 2004), *available at* http://caag.state.ca.us/newsalerts/2004/04-129.htm.

239. Katz v. United States, 389 U.S. 347, 362 (1967).

240. Goldman v. United States, 316 U.S. 129, 135 (1942).

Amendment.[241] In *Katz*, Justice Harlan famously wrote "[*Goldman's*] limitation on Fourth Amendment protection is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[242] By analogy, in *Kyllo v. United States*, the Supreme Court ruled that law enforcement's use of thermal imaging technology to view the interior of a residence[243] was impermissible. In a subsequent case, the Court emphasized the core of *Kyllo*; that the protection of a "legitimate expectation that information about perfectly lawful activity will remain private", and that the technology in *Kyllo* "was capable of detecting lawful activity—in that case, intimate details in a home, such as 'at what hour each night the lady of the house takes her daily sauna and bath.'"[244] Privacy advocates will undoubtedly bear those words in mind when patients, or their prescriptions, are tracked by the new technologies.

C. Error Externalities

There is now some limited evidence of a positive correlation between significant institutional investment in HIT and reduced mortality rates.[245] However, much of the medical literature examining process-supporting HIT has concentrated on failed expectations. In the words of Wears and Berg: "Behind the cheers and high hopes that dominate conference proceedings, vendor information, and large parts of the scientific literature, the reality is that systems that are in use in multiple locations, that have satisfied users, and that effectively and efficiently contribute to the quality and safety of care are few and far between."[246]

There are several possible liability issues for healthcare institutions and health IT suppliers arising from error-reducing technologies. Those issues include institutional failure to introduce the new technologies, transitional problems relating to staff training, the existence of legacy or parallel systems, and system or appliance failures relating to the technologies themselves.[247]

Recent reports suggest that all is not rosy in the garden of error-reducing technologies. Some of this has been apocryphal, with newspaper reports of error-

---

241. *Katz*, 389 U.S. at 362 (1967).

242. *Id.*

243. Kyllo v. United States, 533 U.S. 27, 40 (2001).

244. Illinois v. Caballes, 125 S. Ct. 834, 838 (2005); *Cf.* California v. Ciraolo, 476 U.S. 207, 215 (1986) (no reasonable expectation of privacy from aerial surveillance).

245. Hospitals & Health Networks, 2005 Most Wired Survey and Benchmarking Study, *The Search For Meaning: Does Information Technology Make A Difference?* (2005), *available at* http://www.hospitalconnect.com/hhnmag/jsp/articledisplay.jsp?dcrpath=HHNMAG/PubsNewsArticle/data/0507HHN_CoverStory_Landing_Page&doman=HHNMAG.

246. Wears & Berg, *supra* note 19, at 1261.

247. Terry, *supra* note 156, at 410-13.

prone and physician-unfriendly systems causing problems,[248] while the nation's largest EMR implementation, the Department of Defense's CHCS II system,[249] crashed in the spring of 2004.[250] One estimate suggests that twenty percent of medication errors in 2003 involved automated systems.[251] Not surprisingly, a 2005 Harris Interactive poll reported that sixty-five percent of respondents were either "very concerned" or "somewhat concerned" that "[c]omputerization could increase rather than decrease medical errors."[252]

In the medical literature, there has been little research on the patient safety impact of system-wide EMRs or EHRs. However, Asch et al. report that VHA patients who are covered by a system-wide EMR (and other quality management innovations) experienced higher quality of care than a national sample that did not benefit from such technologies.[253] Reports regarding CPOE and CDSS technologies are far less sanguine and cast some doubts on the effectiveness of these systems.

Perhaps not surprisingly, research suggests reliance on CPOE systems alone will not solve the adverse drug event ("ADE") problem. Nebeker et al. report that while the adoption of CPOE systems has a statistically meaningful impact on input or transcription errors, and tracking technologies reduce administration errors, these technologies do not address ADEs caused by dosing and interaction. More elaborate CDSS technologies are required for that task.[254]

---

248. *See, e.g.*, Charles Ornstein, *California; Hospital Heeds Doctors, Suspends Use of Software; Cedars-Sinai Physicians Entered Prescriptions and Other Orders in it, but Called it Unsafe*, L.A. TIMES, Jan. 22, 2003, at B1; Lisa Richardson, *Kaiser Scrambles to Correct Prescription Mix-Up*, L.A. TIMES, Mar. 18, 2003, at B6; Tracy Weber & Charles Ornstein, *King/Drew Patient Monitors Shut Off Following 2 Deaths*, L.A. TIMES, Sept. 10, 2003, at B1; Ceci Connolly, *Cedars-Sinai Doctors Cling to Pen and Paper*, WASH. POST., Mar. 21, 2005, at A01.

249. Clinical Information Technology Program Office, http://citpo.ha.osd.mil/ChangeNavf9a0.html?SiteNavID=2&PrimNavID=143&SecNavID=180 (last visited Oct. 31, 2005).

250. David Glendinning, *Deploying an EMR: The Battle for Record Access*, AM. MED. NEWS, Mar. 7, 2005, *available at* http://tricare.osd.mil/eenews/downloads/022805CHCSII.doc.

251. Rob Stein, *Automated Systems For Drugs Examined, Report: Computers Can Add to Errors*, WASH. POST, Dec. 21, 2004, at A03.

252. Harris Interactive, *Health Information Privacy (HIPAA) Notices Have Improved Public's Confidence That Their Medical information is Being Handled Properly*, Feb. 24, 2005, at table 5, http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=894 (Expected benefits outweigh risks to privacy; forty-eight percent. Privacy risks outweigh the expected benefits; forty-seven percent). *Id.* at table 6.

253. Steven M. Asch et al., *Comparison of Quality of Care for Patients in the Veterans Health Administration and Patients in a National Sample*, 141 ANNALS OF INTERNAL MED. 938, 938-945 (2004), *available at* http://www.annals.org/cgi/reprint/141/12/938.pdf.

254. Jonathan R. Nebeker et al., *High Rates of Adverse Drug Events in a Highly Computerized Hospital*, 165 ARCH. INTERNAL MED. 1111 (2005); *see also* Anne Bobb et al., *The Epidemiology of Prescribing Errors: The Potential Impact of Computerized Prescriber Order Entry*, 164 ARCH. INTERNAL MED. 785, 788-90 (2004) (suggesting CPOE systems should be matched to CDSS systems to

Garg et al. reviewed trials evaluating the impact of CDSS systems.[255] They reported a trend suggesting improved practitioner performance, but that "the effects of these systems on patient health remain understudied—and inconsistent when studied."[256] One of these unanswered questions is the extent to which physicians will ask for help from a CDSS system or adapt their treatment plans to its recommendation.[257] Miller et al. have raised questions as to the "one size fits all" across sub-disciplines approach of widely available commercial systems and the quality and reliability of the knowledge bases used by these systems.[258]

More disturbing is the finding by Koppel et al. that CPOE systems actually can *facilitate* medical errors.[259] The authors grouped discovered errors into two typologies: "Fragmentation and Systems Integration Failure"[260] and "Human-Machine Interface Flaws."[261] Many of the examples of the former are consistent with the CPOE-CDSS disconnect previously discussed, such as dosage information not interlinked with CPGs. The interface flaws identified included the way CPOE information presentation screen design can lead to the selection of the wrong patient and the use of multiple screens to display all current medications.[262]

Is this merely a transitional phenomenon, or are there more fundamental problems? As Wears and Berg note, "[c]linical work, especially in hospitals, is fundamentally interpretative, interruptive, multitasking, collaborative, distributed, opportunistic, and reactive. In contrast, CPOE systems and decision support systems are based on a different model of work: one that is objective, rationalized, linear, normative, localized (in the clinician's mind), solitary, and single-minded."[263]

---

effectively reduce medication errors).

255. Amit X. Garg et al., *Effects of Computerized Clinical Decision Support Systems on Practitioner Performance and Patient Outcomes: A Systematic Review*, 293 JAMA 1223 (2005).

256. Garg, *supra* note 255, at 1231.

257. *See generally* Charles P. Friedman et al., *Do Physicians Know When Their Diagnoses Are Correct? Implications for Decision Support and Error Reduction*, 20 J. GEN. INTERNAL MED. 334-39 (2005).

258. Randolph A. Miller et al., *Clinical Decision Support and Electronic Prescribing Systems: A Time for Responsible Thought and Action*, 12 J. AM. MED. INFORMATICS ASS'N. 403 (2005).

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

260. *Id.* at 1199-1200.

261. *Id.* at 1200-01.

262. *See also* Jan Horsky et al., *Comprehensive Analysis of a Medication Dosing Error Related to CPOE*, 12 J. AM. MED. INFORMATICS ASS'N 377 (2005).

263. Wears & Berg, *supra* note 19, at 1262 (references omitted).

V. POLICY, MARKETS, AND PRAGMATIC INTERVENTION

A. Introduction

Currently the federal government is attempting to goad the healthcare and IT industries into action with veiled references to carrots and sticks. ONC HIT's Dr. Brailer is reported to believe that there is a HIT market failure,[264] and that the government must do something to prod the industry into action, possibly with loans or extra Medicare reimbursement, to reward EIHR adoption.[265] In the absence of industry agreement on standards, Brailer is reportedly considering a government mandate (presumably along the lines of the HIPAA transactional standards), although he has noted, "Some people think that would be a train wreck, and some people think that would be a great idea."[266] Brailer also stated: "I don't want to see a Son of HIPAA put into law."[267] Secretary Leavitt coined the Bush administration's public, non-regulatory mantra—that the movement to an EIHR should be "a smooth, market-led way,"[268] while Dr. Brailer's public position is that the federal government should act as a "convener" and "catalyst."[269]

There remain, however, significant barriers to EHR adoption occurring without government mandate. According to Ash and Bates, these are technical, organizational (or cultural), and financial.[270] The technical barriers they identify primarily rotate around the well-known issue of interoperability. Organizational barriers include appropriate inclusion of all clinical stakeholders (not just administrators), and the tailoring of technology to physician workflow and time constraints. They identify the primary financial barrier as a "misalignment of resources" facing outpatient practices that cannot recoup investments in new systems.

---

264. Wears & Berg, *supra* note 19, at 1262.

265. Lohr, *supra* note 27.

266. *Id.*

267. Chris Murphy & Marianne Kolbasuk McGee, *Industry Must Improve Its Technology Use*, INFO. WK., June 21, 2004, at 30.

268. HHS, News Release, Secretary Leavitt Takes News Steps to Advance Health IT (June 6, 2005), http://www.os.dhhs.gov/news/press/2005pres/20050606.html.

269. Dr. David T. Brailer, National Coordinator, Health Information Technology, Testimony Before the Committee on Commerce, Science, and Transportation Subcommittee on Technology, Innovation, and Competitiveness, U.S. Senate (June 30, 2005), *available at* http://commerce.senate.gov/pdf/bailer.pdf.

270. *Factors and Forces*, *supra* note 89, at 9-10.

B. Costs and Benefits

Speculatively, a fully operative, national EHR system could reduce the nation's healthcare bill by ten percent, or 1.7 trillion per year.[271] Former HHS Secretary Thompson suggested in July 2004 that health information technology could save $140 billion per year "by reducing duplicative care, lowering health care administration costs, and avoiding errors in care,"[272] while Walker et al. estimated that a fully interoperable EHR could save $77.8 billion annually.[273] In February 2005 the General Accounting Office ("GAO") examined two annual savings estimates widely cited by the Administration ($78 billion from adopting EHRs, $44 billion from adopting CPOEs; both in ambulatory settings). GAO concluded that while "the potential for substantial savings is promising", these estimates were "primarily based on studies with methodological limitations and are contingent on much higher IT adoption rates than are currently estimated[.]"[274]

As is always the case with healthcare expenditures, the actual picture is somewhat more nuanced. First, there are persistent problems with the actuality or timing of substitution of old practices with new technologies. As Chairman Greenspan noted in 2004:

> [W]e know very little about how rapidly medical technology will continue to advance and how those innovations will translate into future spending. To be sure, technological innovations can greatly improve the quality of medical care and can, in theory, reduce the costs of existing treatments. But because medical technology expands the range of treatment options, it also has the potential of adding to overall spending--in some cases, significantly.[275]

Almost all public statements about an interoperable EHR system claim substantial cost savings. Few statements acknowledge, however, that over the next decade the implementation of a national EIHR system could cost as much as $300 billion.[276]

---

271. Lohr, *supra* note 27.

272. HHS, HHS Fact Sheet – HIT Report At-A-Glance, *The Decade of Health Information Technology: Delivering Consumer-centric and Information-Rich Health Care* (2004), *available at* http://www.os.dhhs.gov/news/press/2004pres/20040721.html.

273. Jan Walker et al., *The Value of Health Care Information Exchange and Interoperability*, HEALTH AFF. (2005), *available at* http://content.healthaffairs.org/cgi/content/full/hlthaff.w5.10/DC1.

274. Letter from U.S. Gov't Accountability Office, Health and Human Services' Estimate of Health Care Cost Savings Resulting from the Use of Information Technology 2 (Feb. 16, 2005), *available at* http://www.gao.gov/new.items/d05309r.pdf.

275. Statement of Alan Greenspan, Chairman, Board of Governors of the Federal Reserve System at Hearing Before the House Comm. on the Budget 6-7 (Feb. 25, 2004), http://www.house.gov/budget/hearings/greenspanstmnt022504.htm.

276. Landro, *supra* note 85; *See also* Rainu Kaushal et al., *The Costs of a National Health Information Network*, 143 ANNALS INTERNAL MED. 165 (2005) (estimating $156 billion in capital costs over five year period plus $48 billion in annual operating costs).

C. Financial and Regulatory Intervention Models

Problems of substitution costs and the lack of compelling evidence of positive healthcare outcomes notwithstanding, healthcare policymakers, regulators, and commentators appear to view the interoperable longitudinal EHR as an article of faith in the pilgrimage to safer, more efficient healthcare delivery. Further, although there is still much work to be done at the level of technical standards, it is a reasonably safe assumption that these standards will come to fruition and deliver something like the required level of data coding and interoperability,[277] albeit subject to the privacy and error externalities already discussed. These premises thus beg the question: why are healthcare actors not developing or requesting their vendors to supply interoperable systems?

1. Correcting Market Failure

As already noted, Dr. Brailer's articulated position is that process-supporting technologies have not been implemented in a timely fashion and in quantity because of a market failure in HIT. More specifically, Middleton et al. posit:

> In the current marketplace, in the absence of a similar shared and realizable gain for clinical information exchange, or other recognition of the value of collaboration, there is no incentive from the individual provider's perspective for the adoption and use of a common set of interoperability standards. Viewed from another perspective, by distributing the costs of poor information exchange and interoperability far and wide across all participants in the health care delivery system, each individual entity may be acting rationally from a local perspective, but no entity perceives the magnitude of the lost value in the aggregate. This behavior precludes spending by individual providers or purchasers of HIT for a potential public good dependent upon the cooperation of other independent entities. When the vendors of HIT do not perceive their customers stating interoperability as a requirement of their systems, they act rationally and do not include these features in their products.[278]

---

277. *Cf.* Blackford Middleton et al., *Accelerating U.S. EHR Adoption: How to Get There From Here*, 12 J. AM. MED. INFORMATICS ASS'N. 13, 17 (2005), *available at* http://www.jamia.org/cgi/reprint/12/1/13.pdf [hereinafter *How to Get There From Here*].

> [M]uch more work needs to be done on functional standards for personal health records that interact with EHR systems, inpatient clinical information systems, and additional detail and specification regarding critical functional modules such as provider order entry and clinical decision support.

Id. at 17.

278. *How to Get There From Here*, *supra* note 276, at 14 (reference omitted).

There are two fairly obvious "market failures" at work in the health IT space. First, the interoperable nature of the EHR suggests a fairly classic network effects (or network externalities) problem. Second, the persistent flaw in the United States healthcare market, whereby those who pay for services are divorced from those who consume them, comes into play, resulting in a "misalignment of incentives."[279]

A network effect is "a change in the benefit, or surplus, that an agent derives from a good when the number of other agents consuming the same kind of good changes."[280] The classic example in the economics literature is a telephone service—as the number of users of interoperable telephone equipment increases, so the value of the service to each increases. In the context of an EHR system this "synchronization value,"[281] or benefit, could have two components. First, there may be what is called a direct network effect if, for example, a healthcare provider that pulls EHR data into its EMR system achieves better results (for example, higher satisfaction of patients) or suffers lower costs (for example, a reduction in medical errors). Second, there may be indirect positive network effects if a provider pushes (likely deidentified) data to a central body, resulting in improvements in outcomes research or the reduction of public health costs.[282]

Until there is a critical mass of providers interlinking their EMRs, there is little or no incentive for providers to seek out compatible EMR systems or pay a premium for an EMR with interoperability features; nor do providers have any rational interest in combining with others to build or maintain a health communications infrastructure.[283] The indirect network effect is even more fundamental, as it is difficult to see any near-term economic benefit flowing to the provider who pushes deidentified data to any centralized body.

Even if we project ahead to the EHR tipping point, i.e., when a critical mass of providers are using interoperable EMR systems, the marginal value of interoperability may be very small for a very large, integrated provider that has its own system-wide EMR. Indeed, that marginal value may even be negated by the privacy and security costs associated with "opening" a closed system to national interoperability and the "weakest security link" phenomenon already noted. Similarly, much of medical science, particularly university medical research centers, values the separation of data because of its economic value, suggesting a culture of non-sharing that must be addressed.[284] For these stakeholders,

---

279. *How to Get There From Here*, *supra* note 276, at 14.

280. S. J. Liebowitz & Stephen E. Margolis, *Network Externalities (Effects)*, http://wwwpub.utdallas.edu/~liebowit/palgrave/network.html (last visited Oct. 31, 2005).

281. *Id.*

282. *See generally* Stern School, New York University, Network Effects, http://oz.stern.nyu.edu/io/network.html (last visited Oct. 31, 2005).

283. *See* David J. Brailer, *Interoperability: The Key to the Future Health Care System*, HEALTH AFF. (2005), *available at* https://content.healthaffairs.org/cgi/content/full/hlthaff.w5.19/DCI [hereinafter *The Key To The Future Health Care System*].

284. *See generally* M. L. Baker, *Panel: Cultural Shift Needed to Make Health Data Valuable*, EWEEK,

opening up their internal systems to interoperability also creates a counter-weighing negative externality. Thakor developed a similar hypothesis regarding the financial services sector, further parallels to which are further discussed below, whereby he suggested banks had generally not outsourced their IT or developed interoperable systems because of a belief that maintaining proprietary systems would preserve future strategic options coupled with a desire to exercise control over the sector's IT evolution.[285]

The second major identified failure involves the positive externalities generated when those who invest in new technologies do not receive a satisfactory return on investment. Thus, in the context of healthcare services financing and reimbursement in the United States, it is argued that providers lack incentives to pay for EHR technology, because most of the benefit will accrue to payors.[286] In the future, reimbursement will be more frequently tied to quality or outcomes improvement under "Pay For Performance" ("P4P") programs, potentially giving providers meaningful returns on their HIT investments.[287] However, P4P is still in its infancy[288] and will require additional "pushes" by Congress, such as those found in the *Health Technology to Enhance Quality Act of 2005*.[289]

Ash and Bates make the valuable point that this misaligned incentives problem is exaggerated in the outpatient environment. For example, they argue that while hospitals may recover investments they make in process supporting technologies, the same is not true for outpatient practices, where physicians will make the investment but payers and purchasers will reap almost all of the return on investment.[290] This problem of misaligned resources is not just a theoretical

---

Feb. 19, 2005, *available at* http://www.eweek.com/article2/0,1759,1767127,00.asp.

285. Anjan V. Thakor, *Information Technology and Financial Services Consolidation*, 23 J. BANKING FIN. 697 (1999).

286. *How to Get There From Here*, *supra* note 277, at 14.

287. *Id.*

288. *See*, *e.g.*, Press Release, CMS, Medicare "Pay For Performance (P4P)" Initiatives (Jan. 31, 2005), *available at* http://www.cms.hhs.gov/media/press/release.asp?Counter=1343). *See generally* David A. Hyman & Charles Silver, *The Poor State of Health Care Quality In The U.S.: Is Malpractice Liability Part of The Problem or Part of The Solution?*, 90 CORNELL L. REV. 893, 963-969 (2005).

289. Health Technology to Enhance Quality Act of 2005, S. 1262, 109th Cong. § 301 (2005).

290. *Factors and Forces*, *supra* note 89, at 9-11. *See also How to Get There From Here*, *supra* note 277, at 14:

> [M]any of the patient safety and quality effects of EHRs accrue benefit to the payer or employer–purchaser of health care services who is at greater risk for a patient's total health care costs given decreasing rates of provider reimbursement under capitation. Under fee-for-service reimbursement models, providers have little incentive to use EHRs unless they can contribute enough to practice efficiency or revenue cycle management to improve net revenue per time unit. Under mixed reimbursement models such as variable withholds, and newer pay-for-performance programs, EHRs may contribute to achieving performance or quality benchmarks that warrant increased reimbursement or increased return of withhold payments.

concern. For example, the Community Health Improvement Consortium ("CHIC") of Whatcom County, Washington instituted a pilot e-health system requiring interoperable EMRs and a patient-centric model of care using a web resource and email communication between patients and providers.[291] Hailed as a success by both physician and patient participants as improving quality and reducing overall healthcare costs, the system has not been as popular with physician groups who have seen their income reduced and an inability to recoup their HIT investments.[292] An additional consideration is that there is cogent evidence that hospitals with declining margins are more likely to exhibit increased adverse events,[293] suggesting that those institutions most in need of process-supporting technologies are the least able to finance them.

Applying similar economic models to CPOE/CDSS and track-and-trace technologies reinforces these observations on market failure in EHR provision. Why is this former set of technologies experiencing explosive growth, yet with only minimal (and immature) federal regulatory intervention? First, and most obviously, CPOE/CDSS do not typically require interoperability with other systems and they use standardized platforms such as Microsoft's Mobile/PocketPC operating system (which has a dominant position in enterprises).[294] Second, investment in CPOEs and track-and-trace (and to a lesser extent, CDSS) technologies promises a relatively quick return on investment by reducing medical error low-hanging fruit (such as transcription errors) and reducing losses with tighter inventory and diversion control. Third, the legal system creates incentives for CPOE adoption because: (1) plaintiffs' malpractice attorneys are already able to leverage positive reports in the medical literature and the well-publicized Leapfrog CPOE Standards,[295] (2) at least one state mandates

---

291. Institute for Healthcare Improvement, *Pursuing Perfection: Report from Whatcom County, Washington on Patient-Centered Care*, http://www.ihi.org/IHI/Topics/PatientCenteredCare PatientCenteredCareGeneral/ImprovementStories/PursuingPerfectionReportfromWhatcom CountyWashingtononPatientCenteredCare.htm (last visited Oct. 31, 2005).

292. Gina Kolata, *Health Plan That Cuts Costs Raises Doctors' Ire*, N.Y. TIMES, Aug. 11, 2004, at A1.

293. William E. Encinosa & Didem M. Bernard, *Hospital Finances and Patient Safety Outcomes*, 42 INQUIRY 60, 60–63 (2005).

294. *See generally* Microsoft Windows Mobile, For Business, http://www.microsoft.com/windowsmobile/business/default.mspx (last visited Oct. 31, 2005).

295. *See* The Leapfrog Group, *Factsheet: Computer Physician Order Entry*, Apr. 18 2004, http://www.leapfroggroup.org/media/file/Leapfrog-Computer_Physician_Order_Entry_Fact_Sheet.pdf.

> In order to fully meet Leapfrog's CPOE Standard, hospitals must:
> 1. Assure that physicians enter at least 75% of medication orders via a computer system that includes prescribing-error prevention software;
> 2. Demonstrate that their inpatient CPOE system can alert physicians of at least 50% of common, serious prescribing errors, using a testing protocol. . .; and

CPOE adoption,[296] and (3) the FDA is already in the track-and-trace "business."[297] Finally, in the admittedly limited arena of CPOE adoption, third party payors have been swift to recognize their own interests (improved patient satisfaction and reduced errors) and are either donating handheld devices to large numbers of doctors[298] or rewarding their utilization.[299]

As to EMRs, the market will promote some increases in interoperability when an inevitable consolidation of HIT vendors reduces the number of competing systems, thereby creating some interoperability as more providers use the same system.[300] However, the current market conditions are considerably more complicated than the classic VHS-Beta competition and a "last vendor standing" solution is not likely to appear in the short term (and certainly not within President Bush's target "decade").[301] As a result, most commentators and

---

> 3. Require that physicians electronically document a reason for overriding an interception prior to doing so.

Id. at 2.

296. CAL. HEALTH & SAFETY CODE § 1339.63 (West 2005).

297. Bar Code Label Requirement for Human Drug Products and Biological Products, 69 Fed. Reg. 9120 (Feb. 26, 2004); U.S. Food and Drug Admin., *supra* note 232.

298. *See*, *e.g.*, News Release, Blue Cross Blue Shield of Missouri, New BCBSMO Initiative Jumpstarts Physician Participation in the Electronic Medical Community (Jan.16, 2004), *available at* http://www.bcbsmo.com/wps/portal/chpfooter?PC_7_2_CQ_content_path=shield/noapplication/glabal/news/notertiary/pw_ad033663.htm&RootLevel=&Label=News%20And%20Events (1,700 contracting physicians in Missouri supplied with free handhelds and software).

299. *See*, *e.g.*, Empire Blue Cross Blue Shield, *37 Hospitals Receive Combined Total of $741,200 in Three-Year Patient Safety Initiative*, May 19, 2005, *available at* http://www.empireblue.com/home/press_release/2005/05_19_2005.php (bonuses paid to network hospitals complying that met Leapfrog standard for CPOE and/or ICU staffing).

300. *See*, *e.g.*, Steve Lohr, *I.B.M. Plans to Buy a Health Consulting Firm*, N.Y. TIMES, Apr. 26, 2005, at C3. *See also, Philips to Buy Health-Care Tech Firm*, WALL ST. J., July 7, 2005, at B5 (detailing purchase by Philips Electronics NV of U.S. health-care technology company Stentor Inc. for $280 million aimed at strengthening Philips's position in the U.S. HIT market).

301. Dr. Brailer has framed the issue as follows:

> A central question about interoperability is how it should proceed relative to EMR adoption. Some argue that interoperability has to precede EMR use. They believe that the ability to share information has to be designed into EMRs and that the infrastructure and industry capacity for securely networking this information has to exist up front. They view the risk of widespread adoption of stand-alone EMRs as a lost opportunity and one that may lead irreversibly to treatment of health information as a proprietary asset of delivery systems. They believe that if standards are not solidified and built into EMRs now, a generation of investment will be wasted. Others argue that interoperability will follow from widespread EMR adoption. They believe that once health information is electronic and everyone is using EMRs, interoperability will naturally follow, since it is easier and cheaper than manual data sharing. They view up-front requirements for interoperability as too restrictive and think that standards will naturally evolve from the point-of-care

architects suggest financial incentives of various types, including the availability of government loans or grants to fund hardware and software purchases, and tying reimbursement directly to HIT adoption or indirectly through quality benchmarks.[302]

A study by the Markle Foundation failed to identify a rational business case for the adoption of HIT systems by providers and identified the need for financial incentives for small and medium sized practices in the range $12,000 - $24,000 per full time physician per year, phasing out over time as they were replaced by performance-based incentives.[303] As Middleton et al. note:

> While a great deal of work has been done demonstrating the impact of clinical information systems on clinical decision making and the quality of care, little work has been done that demonstrates the impact of health care information technology on economic outcomes. . . . [T]here is limited solid evidence demonstrating significantly improved financial outcomes resulting from HIT investments.[304]

In a recent development, CMS has announced that it will provide the VA's VistA system free of charge to all doctors,[305] although the details of the plan (particularly the technical and support costs) are not yet known.[306] In September 2005, and after several delays, CMS released an evaluation version of the software, re-designed for doctors' offices, for beta testing and development.[307]

The EHIR "market failure" discourse has concentrated on the HIT market. However, there has been little discussion of the possible impact of IT implementation on the overall healthcare market. Frequently, healthcare is unfavorably compared to the financial services market, primarily because of its comparatively low investment in IT. However, the financial services sector is also an interesting model because of the rapid consolidation it has experienced; consolidation frequently driven by information technologies. Low margin businesses (such as financial and healthcare institutions) that offer commodity products and services require massive scale to continually update their technologies so they can offer new services and a large customer base that they can data mine for marketing purposes; only the largest institutions can afford the

---

> information infrastructure that the United States is building.

The Key To The Future Health Care System, *supra* note 283.

302. *How to Get There From Here*, *supra* note 277, at 15-16.

303. Press Release, Markle Foundation, Connecting For Health Report Analyzes Business Case For Adoption of Health IT Systems (Oct. 22, 2004), http://www.connectingforhealth.org/news/pressrelease_102204.html.

304. *How to Get There From Here*, *supra* note 277, at 13.

305. Gina Kolata, *In Unexpected Medicare Benefit U.S. Will Offer Doctors Free Electronic Records System*, N.Y. TIMES, July 21, 2005 at A14.

306. *Id.*

307. Press Release, Medicare News, CMS Delivers Electronic Health Record Software to Physician Offices, Sept. 19, 2005, *available at* http://www.cms.hhs.gov/media/press/release.asp?Counter=1563. *See also* Vista-Office EHR, http://www.vista-office.org (last visited Nov. 9, 2005).

state-of-the-art technology required.[308] Consolidation occurs in part when financial services institutions invested heavily in IT can leverage their IT investment and expertise to extract value from financial institutions with lesser technologies or expertise.[309]

Dr. Brailer recently testified before Congress, "the gap in EHR adoption between large hospitals and small hospitals, between large and small physician practices, and between other healthcare providers must be addressed. This adoption gap has the potential to shift the market in favor of large players who can afford these technologies, and can create differential health treatments and quality, resulting in a quality gap."[310] A 2005 survey by Hospitals & Health Networks suggests that an IT vector already exists between "Most Wired" and "Least Wired hospitals.[311] For example, in forty-one percent of the most-wired hospitals physicians use CPOEs, compared to only eight percent in the least-wired group (and twenty-seven percent of hospitals nationally).[312] Similar vectors appear in CDSS use (sixty-five percent vs. nineteen percent)[313] and electronic ordering of medications (tweny-eight percent vs. two percent).[314]

However, a "quality gap" could be only one symptom of differential leveraging of HIT; consolidation and driving out of small players may be as likely consequences. Take, for example, the 2005 acquisition of PacifiCare by UnitedHealth for $8.14 billion, a move driven by the change in prescription markets driven by the prescription drug benefit in the *Medicare Prescription Drug, Improvement, and Modernization Act of 2003* ("MMA").[315] If large systems or plans invest heavily in process-supporting technologies, those who do not may be candidates for acquisition. Equally, smaller hospitals or groups that cannot invest in the new technologies may find themselves shut out of relationships with wired providers. As is well known, there has been considerable consolidation of the healthcare industry over the past decade through mergers and, particularly, through hospitals joining systems.[316] Cuellar and Gertler have argued that the quest for efficiencies of scale and leveraging of information systems were less important in driving this activity but concluded "hospital consolidation is likely

---

308. *See generally* Steven Marlin, *Information Technology Spurs Consolidation In Financial Services While Boosting Capacity, Says G-10 Report*, BANK SYSTEMS & TECHNOLOGY, May 1, 2001, *available at* http://static.highbeam.com/b/banksystemstechnology/may012001/informationtech.

309. *See*, *e.g.*, Thakor, *supra* note 285, at 697-700.

310. Dr. David J. Brailer, *supra* note 269, at 6-7.

311. Health & Hospital Networks, *supra* note 245.

312. *Id.* at Figure 1.

313. *Id.*

314. *Id.* at Figure 3.

315. *UnitedHealth to Acquire PacifiCare for $8.14 Billion*, CHICAGO TRIBUNE, July 7, 2005, *available at* http://www.chicagotribune.com/business/chi-0507070173jul07,1,587225.story?coll=chi-business-hed.

316. Alison Evans Cuellar & Paul D. Gertler, *How The Expansion Of Hospital Systems Has Affected Consumers*, 24 HEALTH AFF. 213, 215-217 (2005).

a response to managed care in urban areas, particularly among for-profit hospitals"[317] Worryingly, they report: "Our results show that following consolidation, hospital market power, not the efficiency of care delivery, increased; and hospitals gained higher prices but did not translate them into higher quality of inpatient care or the provision of more community goods."[318]

Several bills introduced in the last two sessions of Congress have sought to provide incentives to HIT and accelerate the development of data interoperability.[319] For example, The *Health Information Technology Act of 2005*[320] would create a competitive "Informatics Systems Grant Program" ($4.05 billion over five years) for most health care providers of up to, for example, $1 million for a critical access hospital or $15,000 for a physician.[321] The proposed legislation would also adjust federal tax law to allow current year deductions of (otherwise capital) informatics expenditures.[322]

The *Health Technology to Enhance Quality Act of 2005* perhaps best suggests Congress' current, bipartisan thinking on how to encourage the adoption of HIT. Co-sponsors, Senators Frist and Clinton, introduced the bill with a statement that it was designed to "encourage creation of an interoperable health IT architecture that fundamentally improves the quality of healthcare, reduces costs and reduces barriers to the adoption of interoperable health IT across all healthcare settings."[323] The bill authorizes five years of $125 million annual matching grants to create local or regional health information plans that promote health information interoperability.[324] Such grants are conditioned on, *inter alia*, the use of the federal standards, privacy standards, and a broad inclusion of stakeholders.

A. Regulation

As described above, in the face of market failure caused by network externalities, a network "owner" can reduce the failure by internalizing some of the network externalities. In the case of the EHR, for example, the federal

---

317. Cuellar & Gertler, *supra* note 316, at 215-217.

318. *Id.* at 217.

319. *See*, *e.g.*, Information Technology for Health Care Quality Act, S. 2907, 108th Cong. (2004); Patient Safety and Quality Improvement Act, H.R. 663; 108th Cong. (2003); Patient Safety Improvement Act of 2003, H.R. 877, 108th Cong. (2003); 21st Century Health Information Act of 2005, H.R. 2234, 109th Cong. (2005); Better Healthcare through Information Technology Act, S. 1355, 109th Cong. (2005).

320. Health Information Technology Act of 2005, S. 1227, 109th Cong. (2005).

321. S. 1227, § 2(e)(2)(A)(ii).

322. S. 1227, § 5.

323. Caroline Broder, *Frist, Clinton to Introduce Healthcare IT Bill*, HEALTHCARE IT NEWS, June 14, 2005. *See also* Press Release, Frist, Clinton Introduce Health Technology To Enhance Quality Act of 2005 (June 16, 2005), *available at* http://frist.senate.gov/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=1961&Month=6&Year=2005.

324. Health Technology to Enhance Quality Act of 2005, S. 1262, 109th Cong. § 201 (2005).

government could internalize the cost of the network infrastructure by building and maintaining it. Similarly, a less obvious "owner," a standards authority such as HL7, may internalize some of the interoperability costs by developing and promulgating messaging standards. The more difficult question, however, is the extent to which government should go beyond cost internalization and drive standards adoption, either directly through regulation of the healthcare industry, or indirectly by dominating or regulating other "owners" such as standards authorities.

A lingering question concerns the core competence of the federal government to create fully functioning, interoperable systems. For example, the Department of Defense's CHCS II medical records system has had problems interoperating with the VA's VistA system,[325] while the IT bioterrorism surveillance systems of the CDC and the Homeland Security Department are years away from interoperable implementation.[326] Not surprisingly, direct federal regulation of patient safety information remains a subject for which few stakeholders seem to show enthusiasm;[327] NCVHS has stayed away from the topic, preferring that the federal government lead by example and as an influential payor.[328] The IOM has seemed closer to accepting that federal regulatory intervention will be required to set data standards.[329] Clearly, the Bush Administration sees regulatory intervention as a last resort (and, possibly, as a tacit admission that its construct has failed).

The reality, of course, is that healthcare is our most regulated industry. It is a domain in which immense public value, intrinsic market failures, and the potential for both financial and physical harms leads to increased regulation on an almost daily basis. Vast areas of health law and regulation continue to reside in our state capitols and, as the federal government continues to offload its financial responsibilities for healthcare to the states, this will only increase.

Only a few examples are needed to demonstrate the pro-regulatory world of modern healthcare and, specifically, HIT. HIPAA is one obvious illustration, but a more recent Bush Administration program is even more telling. The relatively modest electronic prescribing model introduced by the MMA required the establishment of a "Commission on Systemic Interoperability,"[330] amendments

---

325. *See generally* Letter from Linda D. Koontz, Director, Info. Mgmt. Issues, to Steve Buyer, Chairman, Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives (May 14, 2004), *available at* http://www.gao.gov/news.items/d04691R.pdf.

326. Mary Mosquera, *CDC, DHS Years Away from Bioterror, Public Health IT Integration*, GOV'T COMPUTER NEWS, July 11, 2005, *available at* http://www.gcn.com/vol1_no1/daily-updates/36343-1.html.

327. For example, Leape and Berwick pay some regard to regulation (albeit through JCAHO accreditation) and changes in reimbursement, but overall favor payment incentives and disincentives. Leape & Berwick, *supra* note 11, at 2389.

328. Letter from John Lumpkin, *supra* note 103, at 2-3.

329. KEY CAPABILITIES OF AN ELECTRONIC HEALTH RECORD SYSTEM, *supra* note 79.

330. Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA),

to fraud and abuse laws,[331] and regulatory authority to issue electronic prescribing standards.[332] In early 2005, the Center for Medicare and Medicaid Services ("CMS") issued proposed standards for e-prescribing pursuant to the MMA.[333] Although there is no requirement of e-prescribing, if it is used the trading partners must comply with the standards outlined by CMS, specifically the National Council for Prescription Drug Programs SCRIPT Standard (for messaging) and X12N and NCPDP (for eligibility communications).[334]

The recent barrage of proposed federal legislation also suggests that the government will be unable to eschew all regulation of patient safety information. For example, the *Patient Safety Improvement Act of 2003* would have required the federal government to establish standards for outcome reporting,[335] and the *Patient Safety and Quality Improvement Act of 2004* would have promoted and regulated voluntary error reporting of non-identifiable patient safety data by "Patient Safety Organizations," instructed HHS to maintain a national patient safety network of databases, and required the same agency to develop or adopt voluntary standards for interoperability of health information.[336]

In the current term, the proposed *Health Information Technology Act of 2005* would provide federal grants to healthcare providers to aid in the purchase or lease of health informatics hardware and software. Such grants would be conditioned on compliance with the "voluntary" standards on interoperability[337] that the same bill tasks the Secretary to develop within two years.[338] Between 2008 and 2010, such standards would be adopted by DHHS as an "optional" method of receiving reporting data.[339] The *Health Technology to Enhance Quality Act of 2005* would establish a permanent "Standards Working Group"[340] that essentially will take over the Consolidated Health Informatics Initiative.[341] The standards thereafter adopted by HHS[342] would be "voluntary for private

---

Pub. L. No. 108-173, § 1012, 117 Stat. 2066, 2435 (2003).

331. 117 Stat. at §§ 301-307.

332. 117 Stat. at § 108.

333. Medicare Program, E-Prescribing and the Prescription Drug Program, 70 Fed. Reg. 6256 (Feb. 4, 2005) (to be codified at 42 C.F.R. pt. 423).

334. Medicare Program, E-Prescribing and the Prescription Drug Program, 70 Fed. Reg. at 6265.

335. Patient Safety Improvement Act of 2003, H. R. 877, 108th Cong. (2003).

336. Patient Safety and Quality Improvement Act, H. R. 663; 108th Cong. (2003).

337. Health Information Technology Act of 2005, S. 1227, 109th Cong. § 2(f) (2005).

338. S. 1227 § 4.

339. S. 1227 § 4(b).

340. Health Technology to Enhance Quality Act of 2005, S. 1262, 109th Cong. § 2903(a) (2005).

341. S. 1262 § 2903(c).

342. S. 1262 § 2903(e).

entities"[343] but mandatory for the federal government.[344] HHS also would coordinate a certification or accreditation program for hardware, software, and support claiming to comply with the standards.[345]

Even the Frist-Clinton *Health Technology to Enhance Quality Act*, which is the most wired in to current administrative thinking on patient safety information, would (1) require study of the issues and providing grants to cooperative ventures between states,[346] (2) apply HIPAA's privacy, confidentiality, and security provisions to "any health information stored or transmitted in an electronic format,"[347] and (3) amend the Medicare anti-kickback statute[348] and the Stark law prohibition on self-referral[349] to permit payments or support designed to promote the exchange of health information,[350] while requiring HHS to establish a safe harbor for group purchasing of health information technology.[351] As of this writing, the sponsors of the various bills, prompted by encouragement from the Senate Finance and Health Education, Labor, and Pensions Committees have proposed a single compromise bill, to be known as the *Wired for Health Care Quality Act*.[352]

State law examples of patient safety information regulation are legion. For example, California will require acute care hospitals to use CPOEs by 2005,[353] and several states are requiring prescription legibility[354] that inevitably will increase pressure to adopt IT solutions. Further, several states have dramatically increased the reach and complexity of their error and adverse event reporting requirements,[355] with Minnesota's *Adverse Health Care Events Reporting Act of 2003*[356] increasingly being viewed as a model for other states.[357]

California was the first state legislature to consider legislation limiting RFID use because of privacy concerns. Senate Bill 1834[358] would have restricted data collection using RFID to the actual point of sale, thus prohibiting, for example, data collection as the customer browsed through products, or after the customer

---

343. S. 1262 § 2903(f).
344. S. 1262 §§ 2903(e), 2905(b)(1).
345. S. 1262 § 2904(b).
346. S. 1262 §§ 102, 2906.
347. S. 1262 § 2907(1).
348. 42 U.S.C. § 1320a-7(b) (2001).
349. 42 U.S.C. § 1395nn (2001).
350. S. 1262 § 202.
351. S. 1262 § 203.
352. Wired for Healthcare Quality Act, S. 1418, 109th Cong. (2005).
353. CAL. HEALTH & SAFETY CODE § 1339.63 (West 2005).
354. *See, e.g.*, FLA. STAT. ANN. § 456.42 (West 2005).
355. *See, e.g.*, Hospital Report Card Act, 210 ILL. COMP. STAT. 86/25 (West 2005).
356. MINN. STAT. ANN. §§144.706-144.7069 (2003).
357. Angela Galloway, *Hospital-Error Oversight Called Lax*, SEATTLE POST-INTELLIGENCER, May 5, 2005, at A1.
358. S.B. 1834, 2003-04 Sess. (Cal. 2004).

left the store. The bill passed the state Senate, but subsequently was killed by an Assembly committee after objections by business interests.[359] Legislatures in Georgia, Massachusetts, Maryland, Missouri, New Hampshire, New Mexico, Rhode Island, and Utah are either studying the issue, or dealing with bills that contain similar limitations as the California bill, or require disclosure of the existence of a wireless tag or tracking technologies.[360]

HIMSS tracked ninety-eight state bills considered in thirty-seven state legislatures in the first half of 2005.[361] Overall, it seems difficult to imagine that comprehensive federal patient safety information regulation can be avoided. At the very least, diverse state privacy, quality, and patient safety laws will require federal harmonization and, assuming a successful market-led introduction of EIHR, some corrective mechanisms to deal with consolidation of the healthcare market and the financing implications seem inevitable.

VI. PATIENT-CENTRICITY: CAN PRAGMATISM ACCOMMODATE AUTONOMY?

The prevailing view espoused by this country's policymakers and regulators is that patient information (be it transactional or safety related) is to be protected by security and confidentiality. Security keeps out the hackers, and confidentiality (mislabeled by HIPAA as "privacy") keeps the data within the circle of care, thus denying its leveraging for secondary uses such as marketing or patient profiling.

This model is as flawed as it is persistent. What is missing from the picture is real patient *privacy*, an autonomy-based conception that, first, patient information is patient "property" and, second, it is patients who must decide what information should be put into the system, and how and by whom it should be used once it resides there. It may be too late to revisit HIPAA and transactional information; the challenge today is to reframe the patient safety information debate with a patient-centric approach.

These concerns are not the sole province of privacy advocates such as the Electronic Frontier Foundation,[362] but are now more frequently reflected by public opinion. According to a 2005 poll by Harris Interactive, seventy-one percent of respondents knew nothing about the government's HIT plans.[363] When asked to weigh the benefits of an EHR system against its privacy risks,

---

359. Claire Swedberg, *California RFID Legislation Rejected*, RFID JOURNAL, July 5, 2004, *available at* http://www.rfidjournal.com/article/articleview/1015/1/1/.

360. *See* RETAIL INDUSTRY LEADERS ASSOCIATION, 2005 RFID LEGISLATION (2005), *available at* http://www.retail-leaders.org/new/resources/RFID%20Bill%20Summaries%202005%2006-06-05.pdf.

361. Press Release, Healthcare Info. and Mgmt. Sys. Soc'y, All Healthcare IT Legislation Is Local: HIMSS Reviews State Public Policy Focused on Improving Care with Technology (July 14, 2005), *available at* http://www.himss.org/ASP/ContentRedirector.asp?ContentID=65096.

362. *See*, *e.g.*, Electronic Frontier Foundation, Privacy, Security, Crypto & Surveillance, http://www.eff.org/Privacy (last visited Oct. 9, 2005).

363. Harris Interactive, *supra* note 252, at table 4.

respondents were equally divided.[364] Further, forty-two percent of respondents were "very concerned" (and another twenty-seven percent "somewhat concerned") that an EHR system would lead to additional sharing of information without the patient's knowledge.[365]

These issues are not unique to the United States. For example, the United Kingdom, which since 2003 has been working on a national EHR project (*NHS Care Records Service*) as a component of its *National Programme for IT in the NHS*,[366] ran into some serious criticisms and apprehension from providers and patients alike over privacy and security issues.[367] The NHS has published an EHR bill of rights called *The Care Record Guarantee* explaining, for example, the rights of patients to opt out of the system[368] or electronically seal their most sensitive information.[369] Yet, such autonomy is calling into question the value of the overall system plan and the efficacy of treatment given to patients who opt out.

Equally, the Australian *HealthConnect* system, which enjoyed considerable benefits by front-end loading its concept and model with pro-autonomy and pro-privacy principles, has experienced a patient-privacy backlash.[370] As *HealthConnect* has completed its initial trials, it has run into considerable funding and provider participation problems and has continued to raise fundamental questions as to patient privacy and consent.[371] As Commonwealth (federal) funding has slowed, *HealthConnect* is in the process of evolving into a more decentralized and less EHR-centric project that emphasizes point-to-point clinical communication and web-based access to health and health plan information for patients.[372]

The Australian experience suggests that both patients and physicians preferred simple consent models such as a generalized "opt-in" and prospective consent for

---

364. Harris Interactive, *supra* note 252, at table 5.

365. *Id.* at table 5 (Expected benefits outweigh risks to privacy; forty-eight percent. Privacy risks outweigh the expected benefits; forty-seven percent). *Id.* at table 6.

366. National Programme for IT in the NHS, http://www.connectingforhealth.nhs.uk (last visited Nov. 9, 2005).

367. *GPs Fret Over Online Records*, TIMES (London), June 7, 2005, at 6; Sam Lister, *How £6bn Computer System Will Help Heal the NHS*, TIMES (London), Aug. 9, 2004, at 4; Alice Miles, *The Spy in the GP's Surgery*, TIMES (London), Jan. 12, 2005, at 18; Nick Triggle, *Confidentiality Fear Over Records*, BBC NEWS, June 29, 2005, *available at* http://news.bbc.co.uk/2/hi/health/4633213.stm.

368. NHS, *The Care Record Guarantee: Our Guarantee for NHS Care Records in England*, http://www.connectingforhealth.nhs.uk/all_images_and_docs/CRS%20GUARANTEE%20LEAFLET%20%28FINAL%29.pdf (last visited Feb. 9, 2006).

369. John Carvel, *Patients Can Stay Off NHS Database*, GUARDIAN, Jan. 14, 2005, at 11.

370. Terry, *supra* note 77, at 33.

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

372. *See generally* HealthConnect, *HealthConnect Implementation Strategy Version 2.1*, July 6, 2005, *available at* http://www.healthconnect.gov.au/pdf/implementation.pdf. For the most recent version of the Australian EIHR model *see* NEHTA, *Towards an Interoperability Framework: Version 1.8*, Aug. 21, 2005, *available at* http://www.nehta.gov.au/index.php?option=com_docman&task=doc_download&gid=26&Itemid=53.

the pushing of their data to the centralized *HealthConnect* summary record. However, many patients remain uncomfortable with any participation in the system, while providers doubt its efficacy without broad patient participation.[373]

Ironically, the huge difficulty in implementing a true EIHR in the United States may have the effect of perpetuating siloed information, and thereby unintentionally protecting patient privacy and autonomy. For example, system architects continue to be challenged by the question of how the myriad of different healthcare participants should be identified for the purposes of transactional and patient safety networks. Eventually, HIPAA regulations should take care of most of the provider and payor issues through the proposed Identifier Standards.[374] However, any single, social security-like personal health identifier that specifically identifies patients now seems increasingly unlikely.[375] Rather, we should expect far more decentralized, less top-down solutions for identifying specific patients so as to link their records. For example, the Markle Foundation has proposed using record locator (pointer) services or indexes to indicate the location of patient records, or what is known as probabilistic matching based on web search engine technologies that can be used by the current provider to identify prior records pertaining to the patient.[376] Using such approaches necessitates a far less centralized concept of record-keeping and availability. However, it is likely to involve its own error (mistakes in matching) and privacy (a necessity that multiple machine identified records be viewed to confirm the correct match) costs.

There are several (not mutually inconsistent) models (most of which will require regulatory intervention) to make patient safety information systems more responsive to *patient* interests. First, we could adopt a fully autonomy-privacy based model, whereby patients can refuse to allow for certain types of patient safety information acquisition (e.g., RFID tracking) or the inclusion of all of certain types of data (e.g., psychotherapy records) in an interoperable system. Second, a *HealthConnect* type model could be adopted, whereby the patient (in consultation with the relevant physician) determines what summary or excerpted information, if any, is pushed to a centralized record.

Third, an EIHR model could be built that collects (or interconnects) all patient data; but patients and providers determine who can access what information and

---

373. HealthConnect, *Lessons Learned from the MediConnect Field Test and HealthConnect Trials*, Apr. 2005, at 8, *available at* http://www.healthconnect.gov.au/pdf/lessons1-10.pdf.

374. *See, e.g.*, *Notice of Proposed Rule Making for the National Standard Health Care Provider Identifier*, http://aspe.hhs.gov/admnsimp/nprm/npilist.htm; Health Insurance Reform: Standard Unique Employer Identifier, 67 Fed. Reg. 38009 (May 31, 2002) (to be codified at 45 C.F.R. pts 160 and 162).

375. Nancy Ferris, *Hope for Patient ID Dwindles*, GOV'T HEALTH IT, July 11, 2005, *available at* http://www.govhealthit.com/article89517-07-11-05-Web.

376. Markle Foundation, *Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy* (2005), http://www.connectingforhealth.org/assets/reports/linking_report_2_2005.pdf.

for what purposes. Thus, Baker has argued that the prevailing security-centric model for protecting patient information (that she describes as based on authentication, access rules, allowing or denying access, and audit[377]) could be improved upon with a Digital Rights Management ("DRM")[378] style metadata model, whereby the data object (here the patient record) is infused with restrictions on how much of it can be viewed, copied, etc., by any authorized user or class of users.[379] Fourth, and presuming a full-collection EIHR, we could adopt an access-and-edit model, whereby the patient can review the longitudinal record and either delete, restrict access, or seal certain data in an "emergency envelope."[380]

VII. CONCLUSION

Few healthcare stakeholders, the shining exception being JCAHO,[381] accept that patient safety and error-compensation must progress hand-in-hand. Without a broad national consensus on solving our fundamental healthcare quality problems, we will see, at most, only narrow-band reforms. Our policymakers feel boxed in—safety regulation is politically unacceptable because of the country's deep divide over malpractice litigation, while market-based approaches to quality improvement, such as P4P, are at the earliest stages of development. Faced with ever-escalating healthcare costs, the pragmatic solution has been to sidestep the problem by concentrating on technological solutions—which is not a bad thing; HIT is astoundingly powerful and may achieve many of their goals in the long term.

However, the currently articulated HIT models are blinkered by their starting premise that we can only solve the problem with technology at the institutional level, and they sometimes seem unaware of the Orwellian possibilities of their patient safety information construct. There is little doubt that an EIHR fed by

---

377. Dixie B. Baker, Ph.D., Sci. Applications Int'l Corp., Healthcare Info. and Mgmt. Sys. Soc'y, Testimony Prepared for National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentiality 2 (Jan.12, 2005), *available at* http://www.himss.org/content/files/BakerTestimony_FINAL_.pdf.

378. Digital Rights Management (DRM) is an umbrella term referring to any of several technical methods used to control or restrict the use of digital media content on electronic devices with such technologies installed. Wikipedia, Digital Rights Management, http://en.wikipedia.org/wiki/Digital_rights_management (last visited Oct. 31, 2005).

379. Baker, *supra* note 377, at 2-3.

380. For additional suggestions for EIHR privacy models or regulation, *see* Nicolas P. Terry, Testimony before NCVHS Subcommittee on Privacy and Confidentiality, Hearings on Privacy and Health Information Technology: Electronic Health Records and Privacy (Aug. 16, 2005), *available at* http://www.ncvhs.hhs.gov/050816p1.pdf.

381. *See generally* JCAHO, HEALTH CARE AT THE CROSSROADS: STRATEGIES FOR IMPROVING THE MEDICAL LIABILITY SYSTEM AND PREVENTING PATIENT INJURY (2005), http://www.jcaho.org/news+room/health+care+issues/medical_liability.pdf.

technologies such as EMRs, RFID, and CPOE/CDSS technologies will be an unparalleled source of population-based data for health researchers, a potent weapon in the fight against bioterrorism, and a major component in the battle against escalating healthcare costs and unacceptable levels of medical error. But, unless patients and doctors trust HIT systems to respect their privacy and to not introduce additional errors, attempts to overhaul our patient safety information systems will be a failure; doctors will reduce their charting and patients will hide even more information from their doctors.

Federal policymakers and regulators are beginning to recognize that patients and providers must become more closely involved in the EIHR process. Indeed, in a recent speech, Dr. Brailer, who is a true HIT visionary,[382] expressed his desire to be attentive to patient interests with the phrase: "This is not insider baseball."[383] Extending that metaphor, AHRQ Director, Dr. Carolyn Clancy, recently testified before Congress, "[u]nlike the baseball field in the movie Field of Dreams, we have dramatic examples of the building of health IT systems, whose designers found physicians and other clinicians neither came nor played."[384] The likely strategy of the "insiders" is to wait until they have successful regional demonstration projects that suggest compelling cost savings and safety improvements, yet exhibit sufficient levels of confidentiality and security. The problem is that by the time such data exists, the system's concept and architecture will likely be set in a fully interoperable mode that does not allow for opening up summary records or other models more sensitive to issues of autonomy and privacy.

Our patient safety information initiatives must be re-conceptualized as broadly based on error reduction, quality improvement, reasonable compensation, and an unreserved respect for patient autonomy and privacy. Without that consensus, the technical architecture and standards or any HIPAA-style regulatory cram-down that evolve from the current HIT initiatives will be exposed as built on nothing more than sand.

---

382. *See, e.g.*, *The Key To The Future Health Care System*, *supra* note 283.

383. Dr. David Brailer, Keynote Address, American Health Lawyers Association, San Diego (June 27, 2005) (author's contemporaneous notes).

384. Dr. Carolyn M. Clancy, Director, Agency for the Healthcare Research and Quality, U.S. Dept. of Health and Human Servs., Testimony Before the Committee on Commerce, Science, and Transportation Subcommittee on Technology, Innovation, and Competitiveness, United States Senate: Health Information Technology Activities at the Agency for Healthcare Research and Quality (June 30, 2005), *available at* http://commerce.senate.gov/pdf/clancy.pdf.