PERSONAL HEALTH RECORDS: DIRECTING MORE COSTS AND RISKS TO CONSUMERS?*

Nicolas P. Terry **

I. INTRODUCTION

This Article is principally concerned with a subset of Electronic Health Records (EHRs) known as personal health records (PHRs).[1] As the George W. Bush Administration's national EHR project lost some of its momentum due to technical and financial barriers, interest in this more modest, patient-centric model has grown.[2] Mark Rothstein's observation that "the private sector is racing ahead"[3] was confirmed by the 2008 launches of *Google Health*[4] and Microsoft's *HealthVault*,[5] and the considerable press attention they attracted.[6]

** Chester A. Myers Professor of Law, Senior Associate Dean for Faculty, Professor of Health Management & Policy, Saint Louis University, email: terry@slu.edu. My thanks to Tracy Gunter for her thoughtful comments, Margaret McDermott of our law library faculty for her tireless research assistance, and Jessica Flinn, my research assistant, for her detailed research and perceptive editing.

1. The American Health Information Management Association (AHIMA), a non-profit membership association for health information management professionals manages *myPHR*, a consumer information website, that explains the PHR concept and provides links to (but not endorsements of) PHR products and services. American Health Information Management Association, http://www.ahima.org (last visited May 17, 2009); myPHR, http://www.myPHR.com (last visited May 17, 2009).

2. As this article went to press President Barack Obama signed The American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009). As discussed below, the health records financing and privacy provisions in the Act are designed to correct the market failures and legal disincentives surrounding the adoption of electronic medical records. *See infra* Part V.E. Given the timeline for this initiative (records to be available by 2014) and notwithstanding the "soft" regulation of PHRs contained in the stimulus bill, *see infra* notes 176-206 and accompanying text , the new legislation is unlikely to stem the interest in personal health records.

3. Robert Pear, *Warnings Over Privacy of U.S. Health Network*, N.Y. TIMES, Feb. 18, 2007, at 1.22, *available at* http://www.nytimes.com/2007/02/18/washington/18health.html?ex=1187496000&en=c97a17c072836db0&ei=5070 (quoting Professor Mark Rothstein).

4. Google Health, http://www.google.com/health (last visited May 17, 2009).

5. Health Vault, http://www.healthvault.com (last visited May 17, 2009).

6. *See, e.g.*, Catherine Holahan, *Google's Rx for Health Data*, BUSINESS WEEK, Feb. 29, 2008, http://www.businessweek.com/technology/content/feb2008/tc20080229_330594.htm; Craig Stoltz, *Microsoft Health vs. Google Health*, WASH. POST, Mar. 11, 2008, http://www.washing-

In contrast to the more familiar charts, paper records, and electronic medical records maintained by health care providers, PHRs are medical records created and maintained by *patients*. Personal health records are defined as "a single, *person-centered* system designed to track and support health activities across one's entire life experience."[7] PHRs are created by the patient and stored on the patient's personal computer[8] or on a web site[9] provided by the patient's health insurer, health care provider, or employer,[10] the federal government,[11] or even on an independent, commercial site potentially supported by advertising.

The development and adoption of health information technology (HIT)[12] was a familiar, if at times lonely, pillar of the

---

tonpost.com/wp-dyn/content/article/2008/03/10/AR2008031001532.html.

7. THE MARKLE FOUND. CONNECTING FOR HEALTH, THE PERSONAL HEALTH WORKING GROUP, FINAL REPORT 4 (2003), *available at* http://www.connectingforhealth.org/resources/final_phwg_report1.pdf [hereinafter PERSONAL HEALTH WORKING GROUP].

8. For examples of personal software PHRs, see, e.g., MyPro Health Records Organizer, http://www.organizedrecords.com/default.asp (last visited Dec. 17, 2008); WakefieldSoft HealthFile, http://www.wakefieldsoft.com/healthfile/ (last visited Dec. 17, 2008); HealthFrame Applications, http://www.recordsforliving.com/HealthFrame/Applications/ (last visited Dec. 17, 2008); Med-InfoChip.com, http://www.medinfochip.com/ (last visited Dec. 17, 2008); Medical ID from MedicAlert, http://www.medicalert.org/home/Homegradient.aspx (last visited Dec. 17, 2008).

9. For examples of patient subscription web application PHRs, see, e.g., Ingenix, Information is the Lifeblood of Health Care, http://www.ingenix.com/AboutUs/ (last visited Dec. 17, 2008); Press Release, Intuit, UnitedHealthcare, Hewitt Associates, Optima Health and Exante First to Offer Quicken for Health Care (Apr. 12, 2006), http://web.intuit.com/about_intuit/press_releases/2006/04-12.html; Medstory, http://www.medstory.com/ (last visited Dec. 17, 2008); and see generally Caroline McCarthy, *Microsoft to Acquire Search Start-up Medstory*, CNET NEWS, Feb. 26, 2007, http://news.com.com/2100-1032_3-6162108.html.

10. Well–known large corporate employers, hospital systems, and health insurers are implementing PHR systems for their employees and patients. *See, e.g.*, myHealthFolders, https://myhealthfolders.com (last visited Dec. 17, 2008) (web-based health and medical information system offered by BJC HealthCare System); *see also Hospital to Boost Branding with CD-ROMS for Patients*, PHILA. BUS. J., Mar. 28, 2006, http://www.bizjournals.com/philadelphia/stories/2006/03/27/daily12.html (discussing Thomas Jefferson University Hospital's program to distribute medical records software to patients).

11. The Centers for Medicare & Medicaid Services (CMS) launched a pilot program for South Carolina Medicare beneficiaries in April 2008, using software provided by HealthTrio, LLC. Press Release, HealthTrio, LLC, HealthTrio, LLC Personal Health Record Chosen for CMS Pilot for Medicare Beneficiaries (Oct. 15, 2007), http://healthtrio.com/releases/2007/October_15_2007.html. CMS has now announced additional pilot programs for Arizona and Utah. Press Release, CMS Office of Pub. Affairs, Medicare Pilot Program Will Offer Beneficiaries Choices for Maintaining Their Own Personal Records (Aug. 8, 2008), https://www.noridianmedicare.com/phr/pressreleases.htm.

12. *See generally* Nicolas P. Terry, *To HIPAA, a Son: Assessing the Technical, Conceptual, and Legal Frameworks for Patient Safety Information*, 12 WIDENER L. REV. 133 (2005) [hereinafter *To*

Bush Administration's second-term health care agenda. For example, in his 2006 State of the Union address, the President noted, "[W]e will make wider use of electronic records and other health information technology, to help control costs and reduce dangerous medical errors."[13] In 2004 the EHR became the cornerstone of the Administration's HIT policy when the President personally committed to the goal that all Americans would have electronic health records by 2014.[14]

The 2007 and 2008 State of the Union addresses did briefly mention HIT, but not EHRs.[15] Rather, the health proposals in those speeches attempted to build on a first term initiative, the

---

HIPAA, a Son]; Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681 [hereinafter *Ensuring Privacy*].

13. President George W. Bush, State of the Union Address (Jan. 31, 2006), *in* Press Release, Office of the Press Sec'y, President Bush Delivers State of the Union Address (Jan. 31, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/01/20060131-10.html.

14. Whitehouse.gov, Transforming Health Care: The President's Health Information Technology Plan, http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html (last visited May 17, 2009).

The interoperable EHR project was the federal government's third formal foray into e-health. On August 21, 1996, President Clinton signed into law the *Health Insurance Portability and Accountability Act* (HIPAA) of 1996. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of titles 26, 29, and 42 of the United States Code) [hereinafter HIPPA]. The "Administrative Simplification" part of HIPAA included authority for the Department of Health and Human Services (DHHS) to develop standards for HIPAA transactions designed to save hundreds of millions of dollars annually by moving the woefully inefficient U.S. health care system to paperless transactions. *See generally To HIPAA, a Son*, *supra* note 12, at 157-60. During that process DHHS developed privacy and security protections for patient information used in HIPAA transactions. 45 C.F.R. §§ 160, 164 (2007). Not all the pieces of the HIPAA regulatory system were completed when President Bush took office and his administration reduced some patient privacy protections with a revised regulation. For example, 45 C.F.R. § 164.506 (2007) as originally promulgated during the Clinton administration required patient consent for the even routine use by providers, but the subsequent administration removed this requirement. *See* 45 C.F.R. §§ 164.502, 164.506 (2007). The new administration took its own first steps into e-health by authorizing DHHS to develop e-prescribing standards under the Medicare Prescription Drug, Improvement, and Modernization Act of 2003, in part to offset the costs of the Part D prescription drug benefit. *See* Medicare Prescription Drug, Improvement, and Modernization Act of 2003, Pub. L. No. 108-173, § 1201, 117 Stat. 2066 (codified in scattered sections of title 42 of the United States Code) [hereinafter MMA 2003]; *see also* Press Release, Office of the Press Sec'y, State of the Union: Affordable and Accessible Health Care (Jan. 31, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/01/20060131-7.html (discussing President Bush's plan to improve health care).

15. President George W. Bush, State of the Union Address (Jan. 23, 2007), *in* Press Release, Office of the Press Sec'y, President Bush Delivers State of the Union Address (Jan. 23, 2007), *available at* http://www.whitehouse.gov/news/releases/2007/01/20070123-2.html; President George W. Bush, State of the Union Address (Jan. 28, 2008), *in* Press Release, Office of the Press Sec'y, President Bush Delivers State of the Union Address (Jan. 28, 2008), *available at* http://www.whitehouse.gov/news/releases/2008/01/20080128-13.html.

authorization of Health Savings Accounts (HSAs) by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003,[16] with broad (and apparently stillborn) proposals for the deductibility of health insurance premiums by individuals.[17] In other words, further endorsement of Consumer-Driven Health Care (CDHC).[18] The PHR narrative is interwoven with CDHC. In part, PHRs are poised to gain traction because of the numbing financing problems inherent in an EHR model. Related financing issues are behind CDHC and, because they are designed to help consumers understand their own health, and link into published intervention models and their relative costs, PHRs are a crucial enabling technology for CDHC. Both PHRs and CDHC paper-over cracks in our health care and health information technology systems and, in the absence of fundamental reforms such as single-payer or some other model of universal care, both shift costs and risks (albeit different kinds of risks) to patients. This linkage plays out in the legal domain. There, criticisms leveled at CDHC can be leveraged to critique PHRs, and the legal risks associated with PHRs must be added to the list of legal indeterminacies associated with CDHC.

The PHR model is superficially attractive because it seems to lack the "misaligned incentives," network effects, and other market failure problems associated with the financing of a national inter-operative EHR model,[19] while the model's patient-centricity purportedly avoids the privacy-confidentiality-security (PCS) externalities inherent in EHRs. In other words, PHRs are a classic "less-is-more" play.

---

16. MMA 2003, *supra* note 14.

17. *See, e.g.*, President George W. Bush, State of the Union Address (Jan. 28, 2008), *supra* note 15 ("The best way to achieve that goal is by expanding consumer choice, not government control . . . . So I have proposed ending the bias in the tax code against those who do not get their health insurance through their employer. This one reform would put private coverage within reach for millions . . . .").

18. *See generally infra* notes 51-62 and accompanying text.

19. *See generally* David J. Brailer, *Interoperability: The Key to the Future Health Care System*, HEALTH AFF., Jan. 19, 2005, at W5-21, *available at* http://content.healthaffairs.org (In Quick Search Type "Brailer" and "2005"); Blackford Middleton, W. Ed Hammond, Patricia F. Brennan & Gregory F. Cooper, *Accelerating U.S. EHR Adoption: How to Get There From Here*, 12 J. AM. MED. INFORMATICS ASS'N 13, 14 (2005), *available at* http://www.jamia.org/cgi/reprint/12/1/13 (stating that it is the payor or employer-purchaser of health care services who benefits from the patient safety and quality effects of EHRs because they are at greater risk for a patient's total health care costs); *To HIPAA, a Son, supra* note 12, at 171-84; *Ensuring Privacy*, *supra* note 12 at 686 n.20.

The principal thrust of this Article is that, in this case, "less-is-worse;" that PHRs are dangerously flawed adjuncts to or substitutes for provider-centric records, and, while lacking many of the touted quality or cost-reduction benefits of the often-criticized EHRs, they pose substantially higher levels of risk regarding security, privacy, and confidentiality. In a previous article, Leslie Francis and I detailed the privacy and confidentiality issues inherent in a nationwide interoperable EHR model and called for enhanced legal protections to precede its adoption.[20] Contrary to their "less-is-more" positioning, PHRs pose distinct and, in some situations, enhanced risks, requiring a similarly elevated level of legal protection.

Part II examines the stated benefits of PHRs and counters with an examination of their potential flaws or, at least, overstated benefits from the perspectives of patients and physicians. Part III looks at how such a records paradigm might impact quality of care and malpractice litigation, and further examining the linkage between PHRs and CDHC. Part IV analyzes their privacy-confidentiality-security risks, and Part V critically examines some possible legal solutions. The conclusion is that, as with their technically more complex EHR sibling, PHRs require a fundamental reworking of the legal model applicable to *all* electronic health records.

II. ASPIRATIONS, BARRIERS, AND RISKS

The PHR concept is superficially attractive. It offers a route towards large-scale deployment of EHRs at a time when the formal federal government plan seems to be losing some of its momentum. It avoids the classic market failure model that dominates health care changes in the United States, appears to offer a platform upon which information costs associated with CDHC may be reduced, and by placing control of medical information in the hands of patients, aims to avoid the PCS (privacy-confidentiality-security) criticisms leveled at the national, longitudinal EHR.

Further, the potential for PHRs goes beyond functional replacement of a moribund EHR model. PHRs could assert themselves as distinct from CDHC and engage patients in their health and wellness. Additionally, there is considerable

20. *Ensuring Privacy*, *supra* note 12 at 700-07, 730-35.

interest in accelerating the availability of health records to outcomes researchers. Currently, various proprietary and data protection laws create barriers to such "public good" uses of patient data.[21] If providers establish the value proposition of patient sharing of their PHR data by, for example, engineering a feedback loop that facilitates such research flowing back into immediate improvements in individual patient care, then patients may indeed have incentives to create accurate, comprehensive data sets that would be valued by medical researchers (an unlikely development).[22]

In contrast to the financial barriers to EHR adoption, PHRs potentially enjoy an easier ride.[23] First, PHRs are technically simpler than EHRs. They are not fully interoperable and do not suffer from the complexity of industrial-strength EHRs or rely on network effects, whereby incentives to build networked electronic medical records (EMRs) are a function of the existence of other networked EMRs.[24] Second, the incentives to invest in PHR development are well aligned. Experienced IT companies are developing most PHRs with a direct view to the bottom line (whether by sale or from advertising revenue) and an identified market. Patients will purchase PHR services to improve their own health directly, or to better manage a consumer-directed health environment. Employers and health insurers will purchase them for patients to try and reduce their costs by encouraging wellness or facilitating CDHC. Third, the Bush Administration has cited legal indeterminacies (specifically HIPAA's state law savings clause) as a major barrier to a national EHR. In contrast, PHRs are the least regulated form of EHRs, most of their iterations existing in a PCS regulation-free zone.

PHRs are an attractive alternative to the EHR not because they are superior to an EHR, but because they lack most of the

---

21. Nicolas P. Terry, *Legal Barriers to Realizing the Public Good in Clinical Data*, *in* INSTITUTE OF MEDICINE, CLINICAL DATA AS THE BASIC STAPLE OF HEALTH LEARNING: CREATING AND PROTECTING A PUBLIC GOOD (National Institutes of Health, forthcoming 2009).

22. *See infra* notes 43-44 and accompanying text.

23. *See, e.g.*, Lauran Neergaard, *Can PHRs Actually Make You Healthier?* SAN FRANCISCO CHRONICLE, Feb. 5, 2008, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/02/04/national/w120944S71.DTL (noting barriers to EMRs' adoption as driver of PHRs).

24. *See generally* S. J. Liebowitz & Stephen E. Margolis, Network Externalities (Effects) (unpublished article), *available at* http://www.pub.utdallas.edu/~liebowit/palgrave/network.html (explaining that the benefit that can be derived from an item in a network depends on the amount of similar items using that same network).

provider-incurred costs associated with the deployment of the latter. With a PHR model, those costs and risks are shifted to patients. That shift may turn out to be a bad bargain for both patients and their doctors. In this Section, I examine the mainstream operational risks and benefits of PHRs from the perspectives of patients and physicians.

According to the Markle Foundation, PHRs have several distinctive, and impliedly positive, features:

> • **Each person controls his or her own PHR.** Individuals decide which parts of their PHR can be accessed, by whom and for how long.
>
> • **PHRs contain information from one's entire lifetime.**
>
> • **PHRs contain information from all health care providers.**
>
> • **PHRs are accessible from any place at any time.**
>
> . . . .
>
> • **PHRs are "transparent."** Individuals can see who entered each piece of data, where it was transferred from and who has viewed it.
>
> • **PHRs permit easy exchange of information** with other health information systems and health professionals.[25]

For the analysis that follows, these properties are grouped into sets of features (A. Patient Control, Access, and Transparency, and B. Completeness and Interoperability) that are critically observed from the perspectives of patients and providers.

A. Patient Control, Access, and Transparency

With the possible exception of data access or storage being out of control of the patient if a web-based storage system is temporarily (for example, because of network problems) or permanently (for example, the site going out of business) unavailable, a PHR model does indeed suggest patient control,

25. PERSONAL HEALTH WORKING GROUP, *supra* note 7, at 4.

access, and transparency. After all, the patient truly is his or her own data custodian. The fundamental practical flaw in this construct, however, is the assumption that a PHR's value is primarily related to its existence in a patient-controlled silo. No doubt, some patients will construct a limited "silo" database containing, say, lists of medications, account numbers, and providers; data that is never shared outside the patient's own computer. However, the real value of any electronic record, whether personal or not, is in the interoperability of the data. For the patient, that inevitably means acquiring data from or sharing self-generated data with a health care provider, insurer, or pharmacy. Once that decision to share has been made, the control, access, and transparency properties are seriously compromised.

Doctors own the medical records they keep about patients.[26] State statutes have extended that default position to hospital records.[27] HIPAA sought to be agnostic on the issue, purporting to govern only use and disclosure of records.[28] The American Medical Association (AMA) has taken the position that their members should seek to monetize records data.[29] Indeed, a member of the AMA board of trustees has noted that, "there is tremendous economic value to the cumulative data in terms of analyzing patterns," and suggested that control of such data is central to doctors having influence on pay-for-performance programs.[30] Given this background, who will own PHR

26. *See, e.g.*, Waldron v. Ball Corp., 619 N.Y.S.2d 841, 843 (N.Y. App. Div. 1994); Regensdorfer v. Orange Reg'l Med. Ctr., 799 N.Y.S.2d 571, 572 (N.Y. App. Div. 2005); *see also* FLA. STAT. ANN. § 456.057(2) (West 2007) (including "health care practitioner" in definition of "records owner" but excluding, for example, nursing assistants and nursing homes); Am. Med. Ass'n, E-7.04 Sale of a Medical Practice, *available at* http://www.cobar.org/docs/AMA%20(Professionalism) %20E-7.pdf?ID=2373 (discussing conditions for transfer of patient records when selling a medical practice).

27. *See, e.g.*, TENN. CODE ANN. § 68-11-304(a)(1) (West. Supp. 2008); FLA. STAT. ANN. § 456.057 (West 2007).

28. Final Rule, Standards for the Privacy and Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160, 164 (2007)) (Comment and (HHS) Response, Preamble to the HIPAA Privacy Rule); *see also* TRUST in Health Information Act of 2008, H.R. 5442, 110th Cong. § 101-02 (2008) (requiring healthcare providers to obtain informed consent from patients before releasing any medical information to third parties).

29. *See* Kevin B. O'Reilly, *AMA to Set Guidelines on Control of Record Data*, AMNews, Nov. 28, 2005, *available at* http://www.ama-assn.org/amednews/2005/11/28/bisb1128.htm.

30. *Id.* (quoting Dr. William A. Hazel, Jr., a member of the AMA's Board of Trustees). Pay for Performance (or P4P) initiatives are programs that encourage improved quality of care with financial incentives. *See, e.g.*, Press Release, Ctrs. for Medicare & Medicaid Servs., Medicare "Pay For Performance (P4P)" Initiatives, (Jan. 31, 2005), *available at*

data–the patient, the PHR service, or the physician whose services the recorded data relates to? Absent some contractual claim by the PHR service, the patient's ownership of the data seems clear.[31] The problem arises when the patient uploads some or all of his PHR to a physician's EMR. At this point the physician arguably owns this copy of the transferred data.[32]

Physicians may be unwilling to electronically share (download) their records into PHRs, particularly if a third-party web host is seeking to monetize the data. Certainly physicians will not cede control over patient-generated data that they have downloaded into their own patient record system. The patient may have a right of access to[33] and correction of[34] data held by a physician under HIPAA or state law,[35] but that falls well short of "control." Financial institutions see the data sharing inherent in online banking as a marketable "value-add" and as a way of reducing the costs of paper statements and bricks-and-mortar services, but will doctors and their professional organizations see similar benefits?

Practical concerns also intrude. To what extent will patients' requests to download physician-generated data to their PHRs, or to have their own data uploaded to physician EMRs fit the business model of the average doctor's practice? Is this something that the physician will do personally when the patient walks in with a flash drive? Will the time spent performing an upload and/or synchronization ever be reimbursable? Indeed, will doctors charge a separate fee for the requested accommodation in much the same way they are permitted to under HIPAA's access rule[36] and similar state laws?[37]

---

http://www.cms.hhs.gov/ apps/media/press/release.asp?Counter=1343; *infra* text accompanying note 59.

31. *Cf.* Securamed, Frequently Asked Questions, http://www.securamed.com/support_english.med (last visited Dec. 23, 2008) ("Who owns my health record?") (stating explicitly that the data is owned by the patient).

32. *See, e.g.*, FLA. STAT. ANN. § 456.057(1) (West 2007) (including in definition of "records owner," "any health care practitioner to whom records are transferred by a previous records owner"). At this point the physician arguably has ownership rights over the downloaded copy of the patient's data.

33. 45 C.F.R. § 164.524 (2007).

34. 45 C.F.R. § 164.526 (2007).

35. *See, e.g.*, Patient Access to Health Records, CAL. HEALTH & SAFETY CODE § 123100 to 123149.5 (West 2006).

36. 45 C.F.R. § 164.524(c)(4) (2007).

37. *See, e.g.*, FLA. STAT. ANN. § 395.3025 (West 2006); NEB. REV. STAT. § 71-8404 (2003).

B. Completeness and Interoperability

The assertion that a PHR contains information about an entire lifetime and from all health care providers is aspirational, not factual. It is theoretically possible that a patient-centric record could have the same data as a provider-centric longitudinal record, but highly unlikely unless such data was downloaded from a mature, interoperable EHR. Rather, a PHR will only contain the data that the patient is prepared to input or that can be inputted automatically from providers' records.

Doctors are subject to detailed statutory[38] and common law compulsions[39] to keep complete and current records, while federal rules[40] and state statutes[41] are explicit as to how long such records must be retained. It is unclear whether patients' economic or health self-interest will supply anything like the same incentives.[42] The professional responsibility is also long-term. Skepticism is surely merited as to whether patients will show the same diligence throughout an "entire lifetime" or with regard to their relationships with "all health care providers."[43]

It is known that patients routinely lie to their doctors.[44] Will they be more honest when recording their own health infor-

---

38. *See, e.g.*, N.M. STAT. § 61-6-15(D) (2008) ("'Unprofessional or dishonorable conduct' . . includes . . . (33) improper management of medical records, including failure to maintain timely, accurate, legible and complete medical records . . . .").

39. *See, e.g.*, Thomas v. United States, 660 F. Supp. 216, 218 (D.D.C. 1987) (keeping inadequate summary records may constitute malpractice).

40. *See, e.g.*, Condition of Participation: Medical Record Services, 42 C.F.R. § 482.24(b)(1) (2007) ("Medical records must be retained in their original or legally reproduced form for a period of at least 5 years . . . .").

41. *See, e.g.*, LA. REV. STAT. ANN. § 40:2144(F) (2008) (ten years for "Hospital records"); N.M. STAT. § 14-6-2 (2003) (ten years for "all records directly relating to the care and treatment of a patient").

42. There are some reports critical of physician practices regarding data entry in EMRs. *See, e.g.*, Pamela Hartzband & Jerome Groopman, *Off the Record – Avoiding the Pitfalls of Going Electronic*, 358 NEW ENG. J. MED. 1656, 1656-58 (2008).

43. PERSONAL HEALTH WORKING GROUP, *supra* note 7, at 4; *see also* Robert Steinbrook, *Personally Controlled Online Health Data – The Next Big Thing in Medical Care?* 358 NEW ENG. J. MED. 1653, 1655 (2008) (stating that many physicians are wary of increased liability for "incomplete, inaccurate, or difficult to verify" information in personally controlled electronic health records).

44. *See, e.g.*, *Doctors: Patients Who Lie Can be in Danger*, CBS2 CHICAGO, Jan. 20, 2007, http://cbs2chicago.com/health/patients.lying.doctor.2.334683.html; *Patients Lie to Doctors – And Suffer for It*, MSNBC, Feb. 16, 2007, http://www.msnbc.msn.com/id/17188153/.

mation? Will cognitive dissonance or apprehension that another family member might see data on a home computer (or employer or co-worker if on an office machine) result in a selective or edited record? If the PHR is limited to medical expenses and a record of prescription medicines then such issues may not arise (transcription errors aside). Beyond that, patients' lack of technical acumen and medical illiteracy may pose greater problems than honesty, as patients struggle to collect and code (even using "simple" drop-down choices) data.

In practice, patient-created or maintained records will be incomplete and likely inaccurate. At best, they will provide a somewhat distorted "snapshot" or summary record. (In Australia, the summary limitation of the Health*Connect* record was in part responsible for the system's demise.)[45]

The sharing or exchange of data between PHRs and providers or their EMRs is as speculative as it is controversial. The potential for realistic interoperability between PHRs and physician-owned EMRs is unproven.[46] Even assuming that PHRs and EMRs are able to interoperate at some level it is unclear whether that interoperability will have the sophistication (e.g., semantic transparency) or granularity (e.g., specificity of coding) promised by the national EHR project.

Again, the current culture of the physician-patient relationship must be taken into account. It is not difficult to appreciate the kind of dread that a physician must experience when a

---

45. *See* 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), *available at* http://www.jmir.org/2005/1/e3/HTML; *see also* David More, *Health Connect is Dead-So Now What?*, CENTRE FOR POLICY DEVELOPMENT, Feb. 1, 2006, http://cpd.org.au/article/health-connect-dead-so-now-what%3F.

46. So far the most successful initiative regarding such PHR/EMR interconnectivity has been the ASTM/HL7 concord. *See generally* AM. ACAD. OF FAMILY PHYSICIANS' CTR. FOR HEALTH INFO. TECH., ESSENTIAL SIMILARITIES AND DIFFERENCES BETWEEN THE HL7 CDA/CRS AND ASTM CCR 4 (2005), *available at* http://www.centerforhit.org/PreBuilt/chit_ccrhl7.pdf ("HL7 and ASTM have a Memorandum of Understanding (MOU) in place to coordinate efforts to har-monize the CDA and CCR."). Apparently, there was some friction between ASTM (CCR) and HL7 (with its CDA) as to whether these were competing standards. Jack Beaudoin, *ASTM, HL7 Struggling to Get Along*, HEALTHCARE IT NEWS, Aug. 18, 2004, http://www.healthcareitnews.com/news/astm-hl7-struggling-get-along. However, by 2007 the two organizations had harmonized CCR and CDA into a single standard, known as the "Continuity of Care Document" (CCD). Press Release, Health Level 7, Inc. and ASTM International, HL7 Continuity of Care Document, a Healthcare IT Interoperability Standard, is Approved by Balloting Process and Endorsed by Healthcare IT Standards Panel (Feb. 12, 2007), *available at* http://www.hl7.org/documentcenter/public/pressreleases/20070212.pdf.

patient walks into his consulting room armed with a sheaf of printouts from Internet medical advice and pharmaceutical marketing web sites.[47] Will the PHR-equipped patient now begin that encounter by presenting his or her "record"? Will the physician see this as an opportunity to work with a well-informed patient vested in shared responsibility for his or her health care, or view it as another indication of the deterioration of professional hegemony as patients, health care institutions, and commercial entities struggle to become the dominant players in the health care encounter?

Finally, given the overall patient-centricity value proposition of the PHR, we must acknowledge again its greatest medico-legal Achilles' heel. Most of the important patient-centric attributes of the PHR (control, access, and privacy) assume that the PHR data will remain in a patient-controlled silo. Yet, as soon as the data is shared with a physician it is no more "personal" or personally controlled than any other piece of verbal or written data put in the hands of the physician. Once it is absorbed into the doctor's EMR, the data (or at least that copy or version) is no longer practically or legally in the patient's control.

In the next three Parts, I place these patient and physician concerns in a legal frame, looking first at quality risks and quality of care litigation issues, and then PHR privacy-confidentiality-security risks, and some potential solutions.

III. SHIFTING QUALITY RISKS; CHANGING LIABILITY MODELS

As follows from the above discussion, the PHR model involves patients incurring some medical records costs. This is not a simple shift of costs from health care providers to patients; after all, providers will still keep their own EMRs. Notwithstanding, the more ambitious scheme of EHR interoperability founders, PHR substitution will (near-term at least) shift costs to patients. "Cost" is not a simple concept in this context. Some patients will no doubt purchase PHR software

47. *See generally* Nicolas P. Terry, *Prescriptions sans Frontières (or How I Stopped Worrying About Viagra on the Web but Grew Concerned About the Future of Healthcare Delivery)*, 4 YALE J. HEALTH POL'Y L. & ETHICS 183 (2004) (describing how the Internet has transformed the prescribing and dispensing of medications to patients, and arguing that a careful balance must be struck between regulating web-based prescription services and supporting greater autonomy for consumers to knowledgeably control their own healthcare).

or a PHR web subscription, but most will be provided with "free" PHRs. Many of these will be explicitly advertiser-supported or financed by leveraging the patient's hosted data in some other way. Finally, patients supplied with PHRs by employers or insurers may incur distinct PCS costs. However, the potential patient and, as will be seen, provider-incurred costs discussed in this section are of a different character. How will the implementation of PHRs affect, negatively or positively, the quality of the patient's care? And, how might PHRs influence the nature or quality of care litigation?

A. PHRs and Health Quality

There are several avowed, quality-related reasons for investing in a wide-scale (e.g., regional or national) interoperable EHR. Such systems have the potential to enable related quality-improving and error-reducing technologies such as CPOE (computerized physician order entry), CDSS (clinical decision support system), and other surveillance systems, facilitate accurate and legible communication among providers, automate adverse event and medical error disclosure, and provide for reliable and reproducible outcomes research and reporting.[48] EHRs, therefore, are designed to produce both *individual* health and *population-wide* improvements to the quality of health care.

In contrast, PHR contribution to the health of the individual patient keeping the record is difficult to evaluate. Clearly it will not have the impact of EHR data in a mature HIT environment where EHR data will be integrated into a provider's CDSS and surveillance systems.[49] Nevertheless, a reasonable PHR should have some "wellness" benefits and is likely to have some "alarm" settings for dosages and interactions of currently prescribed drugs.

---

48. *See generally* Gunter & Terry, *supra* note 45 (evaluating the benefits and challenges of two proposed national electronic health record models (American and Australian), and the various ways centralized and systematized data will transform the nature of medical records collection and storage); *see also Access To Electronic Medical Records Significantly Increases Efficiency of Emergency Care*, SCIENCEDAILY, May 30, 2008, http://www.sciencedaily.com/releases/2008/05/080530074313.htm (discussing reduction in costs in treating emergency room patients with EMRs by, for example, avoiding extraneous medical tests).

49. *See generally To HIPAA, a Son*, *supra* note 12, at 138-47 (stating how hospitals and other in-patient care facilities will utilize "tracking" and "tracing" technologies to monitor every detail of a patient's condition while inside the health care facility).

However, it is unclear how PHRs can serve *any* population-wide or public health law goals. Indeed, their patient-centric value proposition seems antithetical to any public benefit. No doubt some PHR-generated data will escape into public or private research domains; some PHR providers may simply sell patient data to researchers while the more careful and ethical ones will navigate the limited PCS issues with contractual consents or sell only de-identified data. And, of course, PHR data that is absorbed into an EMR will be treated as any other research data, subject to known PCS constraints. Overall, however, data held exclusively in PHRs will have only a marginal impact on health outcomes research or epidemiological studies.[50]

B. Consumer-Directed Health Care

The PHR narrative is inextricably linked to proposals for consumer-directed health care. The first linkage is economic because the same fundamental health care financing problems (market failures, misaligned incentives, etc.) underlie both proposals. The second link is that CDHC is heavily reliant on major decreases in consumer information costs. PHRs containing individual health data and linking out to generalized wellness and treatment information may play a crucial enabling role for CDHC. As a result, criticisms leveled at CDHC provide an additional stick with which to beat its new fellow traveler, while the specific practical and legal problems associated with PHRs (issues that go beyond concerns about EHRs) cast additional critical light on CDHC.

The components of CDHC are as well-known, as they are complex and controversial.[51] "Consumer-directed health

50. Some have argued further that empowering patients to control and maintain their longitudinal records will result in an injurious shift of patient data from academic research institutions to companies new to the health care enterprise. *See* Kenneth D. Mandl & Isaac S. Kohane, *Tectonic Shifts in the Health Information Economy*, 358 NEW ENG. J. MED. 1732, 1732-37 (2008).

51. *See* TIMOTHY STOLTZFUS JOST, HEALTH CARE AT RISK: A CRITIQUE OF THE CONSUMER-DRIVEN MOVEMENT 17-26, 119-49 (Duke Univ. Press 2007) [hereinafter HEALTH CARE AT RISK]; *see also* Mark A. Hall & Clark C. Havighurst, *Reviving Managed Care with Health Savings Accounts*, 24 HEALTH AFF. 1490, 1492 (2005) ("Despite . . . question marks, the strategy of causing consumers to set aside assets for spending on their own health care should inspire at least some economizing behavior of the sort that has been systematically missing with comprehensive first-dollar coverage. It may also help increase patients' awareness that medical care

plans" (CDHPs), that couple catastrophic insurance coverage with large deductibles, are designed to replace traditional employer-funded health insurance.[52] Consumers, out of their own tax-sheltered health savings accounts, will pay for non-catastrophic costs.[53] The newly empowered patient as consumer, so we are told, will hungrily and efficiently seek out health quality data available on federal[54] and state web sites[55] prior to selecting a provider, accept more personal responsibility for his or her health and health care, rely more on health information from commercial[56] or provider web sites,[57] and maintain his or her own personal health record.[58] Faced with such informed and empowered consumers, providers will have to compete on both price and quality while receiving additional "market-leading" incentives from pay-for-performance (P4P) programs instituted by managed care organizations and the federal government.[59] CDHC is designed to move health care costs to patients in order to reduce health care consumption (and moral hazard issues) and with the hope that

---

costs real money and thus diminish the extreme entitlement mentality that affects most people's attitudes toward health care.").

52. *See* UNITED STATES GOV'T ACCOUNTABILITY OFFICE, CONSUMER-DIRECTED HEALTH PLANS: SMALL BUT GROWING ENROLLMENT FUELED BY RISING COST OF HEALTH CARE COVERAGE 2 (2006), *available at* http://www.gao.gov/new.items/d06514.pdf.

53. A related proposal was President Bush's 2007 State of the Union tax deduction proposal to tax workers for their health benefits, but provide a health insurance deduction for any individuals with health insurance. President George W. Bush, State of the Union Address, *supra* note 15. This plan, which seems to have garnered little political traction, has been criticized as a tax benefit for the wealthy, as ineffective to reduce the number of uninsured (few of whom have any tax liability), and likely to erode employer-provided health care insurance. *See, e.g.*, Karen Davis, *The 2007 State of the Union Address: The President's Health Insurance Proposal Is Not a Solution,* THE COMMONWEALTH FUND, Feb. 1, 2007, http://www.commonwealthfund.org/Content/From-the-President/2007/The-2007-State-of-the-Union-Address--The-Presidents-Health-Insurance-Proposal-Is-Not-a-Solution.aspx.

54. *E.g.*, Medicare, Nursing Home Compare, http://www.medicare.gov/NHCompare/ (last visited Dec. 20, 2008).

55. *E.g.*, Virginia.gov, Virginia Board of Medicine Practitioner Information, http://www.vahealthprovider.com (last visited Dec. 20, 2008).

56. Nicolas P. Terry, *Cyber-malpractice: Legal Exposure for Cybermedicine*, 25 AM. J.L. & MED. 327, 327-66 (1999).

57. Milt Freudenheim, *AOL Founder Hopes to Build New Giant Among a Bevy of Health Care Web Sites*, N.Y. TIMES, Apr. 16, 2007, at C1.

58. *See generally* Gunter & Terry, *supra* note 45 (describing personal EHRs); *Ensuring Privacy*, *supra* note 12, at 681-735 (discussing that a nationwide electronic health record system "must embrace an autonomy-based, default position of full patient control over personal information, with very limited exceptions.").

59. *See, e.g.*, Medicare "Pay For Performance (P4P)" Initiatives, *supra* note 30.

market forces will drive down health care costs so that it becomes affordable for the 47 million uninsured Americans.[60]

For CDHC to evolve from a slogan concealing additional cost and risk-shifting to patients, into a new paradigm of rational health care consumption, requires a radical reduction in patient-incurred information costs. The CDHC model assumes that most consumer information will be sourced from providers and that this will be supplemented by information from government and commercial web sites.[61] The barriers to reductions in patient information costs are numerous. Many, if not most, patients suffer from medical and economic illiteracy.[62] As more information is provided to them they will incur significant sorting costs. Further, there are major practical barriers to any type of information processing during times of crisis, such as during an emergency admission.

PHR data likely will function as a source of patient information. The process of maintaining a PHR could engage the patient more fully in his health care status. Some PHRs will link rich data to patient-reported conditions or physician-reported diagnoses. At some level, therefore, PHRs potentially will enable CDHC. What is unknown, at the present, is whether PHRs will reduce information costs and make CDHC more workable or whether PHRs will operate as a type of Trojan horse, falsely convincing consumers that they are in charge of their health care and so making CDHC more palatable.

---

60. *See, e.g.*, STAN DORN, URBAN INST., UNINSURED AND DYING BECAUSE OF IT: UPDATING THE INSTITUTE OF MEDICINE ANALYSIS ON THE IMPACT OF UNINSURANCE ON MORTALITY 2-3 (2008), *available at* http://www.urban.org/UploadedPDF/411588_uninsured_dying.pdf (estimating excess mortality due to lack of insurance at 137,000 people from 2000-2006 and approximately 22,000-27,000 people in 2006).

61. *See* CONSUMER-DIRECTED HEALTH PLANS, *supra* note 52, at 2.

62. *See, e.g.*, SHEIDA WHITE, AM. MED. ASS'N FOUND., ASSESSING THE NATION'S HEALTH LITERACY: KEY CONCEPTS AND FINDINGS OF THE NATIONAL ASSESSMENT OF ADULT LITERACY (NAAL) 43 (2008), *available at* http://www.ama-assn.org/ama1/pub/upload/mm/367/hl_re-port_2008.pdf (discussing how more than one-fifth of adults have a basic or below level of health literacy); INST. OF MED., HEALTH LITERACY: A PRESCRIPTION TO END CONFUSION 2 (2004) ("Forty million Americans cannot read complex texts . . . at all, and 90 million have difficulty understanding complex texts. Yet a great deal of health information, from insurance forms to advertising, contains complex text."); AGENCY FOR HEALTHCARE RESEARCH & QUALITY, LITERACY AND HEALTH OUTCOMES 1 (2004), *available at* http://www.ahrq.gov/clinic/epcsums/litsum.pdf ("Low literacy is common in the United States; a decade ago, 40 million adult Americans scored on the lowest of five levels (level 1) of the National Adult Literacy Survey (NALS); another 50 million scored at level 2.").

C. Liability Indeterminacies and CDHC

Our traditional health care liability systems are premised on a financing-agnostic model. That is, the financing of a medical procedure generally is insulated from the liability rules that assess any resulting adverse events and influence its quality. This is true regarding both the custom (physician-centric) standard of care in diagnosis or treatment cases[63] and the expectations (patient-centric) standard used by a slight minority of jurisdictions in informed consent cases.[64] Courts have generally brushed back theories of liability where patients have sought to intermingle their personal financial situations with medical decision-making.[65] While, shamefully, lack of insurance may justify a provider refusing to treat a patient at all,[66] the courts have taken the position that, once there is a physician-patient relationship, treatment must be rendered regardless of financing concerns.[67] Of course, the numbingly complex managed care ERISA[68] litigation that began in the mid-1990s put a related issue front and center as patients brought

---

63. *See generally* Morrison v. MacNamara, 407 A.2d 555, 560-65 (D.C. 1979); Hall v. Hilbun, 466 So. 2d 856, 870 (Miss. 1985); Morgan v. McPhail, 672 A.2d 1359, 1362 (Pa. Super. Ct. 1995).

64. *See* Canterbury v. Spence, 464 F.2d 772, 780 (D.C. Cir. 1972) ("True consent to what happens to one's self is the informed exercise of a choice, and that entails an opportunity to evaluate knowledgeably the options available and the risks attendant upon each. The average patient has little or no understanding of the medical arts, and ordinarily has only his physician to whom he can look for enlightenment with which to reach an intelligent decision. From these almost axiomatic considerations springs the need, and in turn the requirement, of a reasonable divulgence by physician to patient to make such a decision possible."), *cert. denied*, 409 U.S. 1064 (1972).

65. *See, e.g.*, Arato v. Avedon, 858 P.2d 598, 608 (Cal. 1993) (holding that informed consent duty owed to cancer patient did not include a duty to advise patient of risks of failing to put his estate into good order).

66. *See, e.g.*, Birmingham Baptist Hosp. v. Crews, 157 So. 224, 225 (1934); *see also* Childs v. Weis, 440 S.W.2d 104 (Tex. App. 1969).

67. *See, e.g.*, Muse v. Charter Hosp., 452 S.E.2d 589, 594 (N.C. Ct. App. 1995); *see also* Wickline v. State, 239 Cal. Rptr. 810, 819 (Cal. Ct. App. 1986) ("a physician who complies without protest with the limitations imposed by a third payor, when his medical judgment dictates otherwise, cannot avoid his ultimate responsibility for his patient's care."); Ricks v. Budge, 64 P.2d 208, 211-12 (Utah 1937) (discussing physician's on-going duties following treatment).

Also noteworthy is The Emergency Medical Treatment and Active Labor Act (EMTALA), 42 U.S.C. § 1395 (2000), which requires Medicare-participating hospitals to offer emergency services to "provide for an appropriate medical screening examination within the capability of the hospital's emergency department," and can lead to duties to stabilize. EMTALA protects against discriminatory treatment of uninsured or impecunious patients. *See generally* Morgan v. N. Miss. Med. Ctr., Inc., 458 F. Supp. 2d 1341 (S.D. Ala. 2006).

68. Employee Retirement Insurance Security Act of 1974, Pub. L. No. 93-406, 88 Stat. 832 (codified as amended at 29 U.S.C. §§ 1001-1461 (2000)).

legal challenges to the coverage decisions of managed care entities.[69] However, the basic proposition of cost/financing agnosticism survived the "ERISA decade;" once treatment has been undertaken, a dispute over the quality of care is a separate, non-ERISA issue.[70]

What, however, will be the response of the courts to quality of care issues when the patient is financing some or all of his own care (e.g., paying for it from an HSA) and, as a result, inevitably making decisions that will relate to the quantity or quality of care? Haavi Morreim has argued that the courts will be faced with actions premised on informed consent theories that allege failure to adequately warn of the cost of procedures; while providers will make increased use of affirmative defenses, such as assumption of risk and comparative negligence, against patients whose own financial decisions influenced the mode of treatment.[71] Certainly some jurisdictions have extended the risk-disclosure duty to cover situations where the patient refuses treatment,[72] suggesting the need for a complex dialogue between the frugal patient and the ethically and legally constrained physician. Affirmative defenses, on the other hand, may not be as readily applicable. Courts have stepped up their pressure on patients to cooperate with their treating physicians and obey post-treatment instructions. As noted by the Supreme Court of New Jersey:

> [O]nce the patient comes under the physician's care, the law can justly expect the patient to cooperate with the health care provider in their mutual interests . . . [and] it is not unfair to expect a patient to help avoid the consequences of the condition for which the physician is treating her.[73]

---

69. *See, e.g.*, Pegram v. Herdrich, 530 U.S. 211 (2000); Rush v. Moran, 536 U.S. 355 (2002).

70. *See generally, e.g.*, Petrovitch v. Share Health Plan of Ill., Inc., 719 N.E.2d 756 (Ill. 1999) (Patient brought suit against HMO, alleging that it was vicariously liable for the conduct of her participating treating physician after cancer treatment was already undertaken. The suit was not brought under ERISA, and the court found that an HMO can be held vicariously liable for the negligence of physicians.).

71. E. Haavi Morreim, *High-Deductible Health Plans: New Twists on Old Challenges from Tort and Contract*, 59 VAND. L. REV. 1207, 1207-61 (2006).

72. *See, e.g.*, Truman v. Thomas, 611 P.2d 902, 906 (Cal. 1980) (holding that a physician is obligated to provide his patient with all information material to her decision to refuse a pap smear).

73. Ostrowski v. Azzara, 545 A.2d 148, 156 (N.J. 1988).

However, these mitigation or "avoidable consequences" types of cases aside, the courts have tended to reject affirmative defenses based on pre-treatment conduct or circumstances in large part because the physician must treat the patient as he presents.[74] Given the informational asymmetry between patient and provider, the subjective standards traditionally applied to the affirmative defense inquiry, and sometimes-applicable duties to treat notwithstanding lack of insurance,[75] courts may not be eager to penalize patients because of their financial circumstances or any treatment decision "they" made.

Notwithstanding, Peter Jacobson and Michael Tunick have argued, "it seems likely that legal doctrine will evolve in ways that permit physicians to take costs into account without vulnerability to medical liability."[76] However, they also predict novel areas of provider exposure; for example, the supply of inaccurate or outdated cost and quality information to patients.[77] Finally, Timothy Jost weighs in with an appropriate summary: "All that can be said for certain is that the relationship between patients and providers will change in ways that are not now fully predictable and that professionals and patients may not like."[78]

D. Adding PHRs to the Legal Mix

This growing literature concerning the legal indeterminacies of CDHC can be downloaded into the PHR debate. PHRs not only enable CDHC, but also involve their own, additional level of privatization of health care (the shifting of records burdens and risks from government, employers, and providers to individuals).

A provider-centric liability model is premised on physician-held patient data. In exploring the rationale for privacy and confidentiality I have noted the traditional, albeit tacit, under-

74. *Id*. at 152. *See also* Bryant v. Calantone, 669 A.2d 286, 289 (N.J. Super. Ct. App. Div. 1996).

75. *E.g.*, Emergency Medical Treatment and Active Labor Act of 1985, 42 U.S.C. § 1395dd (2006).

76. Peter D. Jacobson & Michael R. Tunick, *Consumer-Directed Health Care and the Courts: Let the Buyer (and Seller) Beware*, 26 HEALTH AFF. 704, 708 (2007).

77. *Id*. at 710.

78. HEALTH CARE AT RISK, *supra* note 51, at 160.

standing providers and patients have regarding the provider being the sole custodian of medical information: "patients provide information to physicians in the belief that it will further their diagnosis and treatment while physicians respect confidences in order to encourage patients to disclose personal and medical information that will make diagnosis and treatment more effective."[79] However, the PHR model disrupts this understanding. Two "sets of books" will be kept, the patient's PHR, and the doctor's records (whether electronic or not). Will they contain the same information? Will the patient, now the guardian of his own medical information, disclose his entire PHR? If so, will the physician be able to cope with the sorting costs of being presented with a voluminous, parallel personal record? Will the standard of care be adjusted to allow for physician reliance on patient-entered data? And will the physician be under a duty to "return the favor" and add "his" data to the patients' PHR in anticipation of the patient's next encounter with a health care provider?

PHRs create their own share of legal indeterminacies. As PHR data becomes a major predicate for CDHC (patients making decisions on the basis of cost taking into account their own data set), will that decrease provider liability or open up new allegations of negligent behavior by providers? For example, will the standard of care be adjusted to reflect physician reliance on PHR data?

IV. INCREASED PRIVACY, CONFIDENTIALITY, AND SECURITY RISKS

At first sight, and particularly if you agree philosophically with CDHC, PHRs seem to offer some real advantages over a national EHR system. They seem to avoid the financing challenges of EHRs (being both technically more modest and less victimized by market failures) while providing an end-run around patient and physician concerns about the privacy, confidentiality, and security of electronic records. Indeed, as noted above, the Markle Foundation has described PHRs as "private and secure."[80] In this section I argue that the privacy

79. Nicolas Terry, *What's Wrong with Health Privacy?*, *in* LAW AND BIOETHICS 68, 73 (Sandra H. Johnson, Ana S. Iltis & Barbara A. Hinze eds., Routledge, 2008) [hereinafter *What's Wrong with Health Privacy*].

80. PERSONAL HEALTH WORKING GROUP, *supra* note 7, at 4.

and security benefits of PHRs are largely illusory and that the PCS legal protections are considerably less robust than those for the EHR (which itself poses severe problems).

A. Medical Data at Risk?

Press stories about data breaches involving medical information are legion.[81] Perhaps none is more famous than the Veteran's Administration's (VA) misplacement of the unencrypted names, birthdates, and Social Security numbers of 19.6 million to 26.5 million veterans contained on a laptop stolen from a VA employee's home.[82] A recent study by a privacy advocacy group pointed to 291 publicly reported data breaches involving personal health information in the period between the effective date of the HIPAA privacy rule (April 2003) and the end of 2007.[83] These breaches potentially exposed the medical data of more than 16 million individuals.[84]

B. PHR Data at Risk?

If PHRs are created and managed by patients themselves, how can they be at PCS risk? Certainly, there would seem to be few privacy and confidentiality risks if the data is stored on the patient's home computer. There may be security risks if the patient's computer is hacked or the patient loses the USB drive to which he has exported his unencrypted data, but these are hardly issues peculiar to medical information or fertile ground for legal intervention.

Considerably more risks arise if the patient is using a web-based PHR service because the patient no longer has physical control over the data.[85] What guarantees does the patient have

---

81. *See, e.g.*, *Ensuring Privacy*, *supra* note 12, at 684 n.7. There is even a web site now devoted to chronicling data breaches (only some of which relate to medical information). Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited May 17, 2009).

82. *See* Christopher Lee, *VA Knew Early About Data Theft, Officials Did Not Tell Secretary for 13 Days, Document Shows*, WASH. POST, May 27, 2006, at A4, *available at* http://www. washingtonpost.com/wp-dyn/content/article/2006/05/25/AR2006052501237.html.

83. POGOWASRIGHT.ORG, MEDICAL PRIVACY AT RISK: A CALL FOR EFFECTIVE LEGISLATION 3 (2007).

84. *Id.*

85. Compare inherent web risks, for example: cookie-based traffic data or other consumer profiling.

that the data is secure or that it will not be shared with third parties? First, assume that the service provider has a prior relationship with the patient; for example a health insurer, employer, or health care provider. What guarantees does the patient have that the data he or she enters will not be used to further some other goal of the service purchaser, such as an employer looking to promote only employees who are in wellness programs? Second, assume that the service provider has no such relationship but seeks to monetize the information it collects by selling the data it collects to advertisers (e.g., a smoking cessation plan marketed to PHR subscribers who check the "smoker" box).

Given their current low penetration of the records market, it is impossible to gauge the type or level of PCS risks that PHRs will incur.[86] What we do know is that the pharmaceutical industry spends $25-$30 billion annually on marketing, more than twice their expenditure on research and development.[87] With such large stakes in play it seems reasonable to assume that data aggregators and data mining services will be interested in having some access to PHR data and that the providers of PHR services will be interested in creating a revenue stream from either providing the data directly, or leveraging it to encourage targeted DTC (direct-to-consumer) advertising by drug companies.

Finally, an obvious factual circumstance must be addressed; one that at the very least will confuse patients attempting to comprehend the legal protection of their PHR data. In the words of a 2007 study performed for The Office of the National Coordinator for Health Information Technology (ONCHIT):[88]

> What we do note is that PHRs contain much of the same information covered by HIPAA, even if the PHR vendor is not itself a HIPAA-covered entity. It would appear to be an inconsistency in the legal framework to

86. CAL. HEALTHCARE FOUND., SNAPSHOT, THE STATE OF HEALTH INFORMATION TECHNOLOGY IN CALIFORNIA 21 (2008), *available at* http://www.chcf.org/documents/chronicdisease/ HITSnapshot08.pdf (noting only two percent of Californian consumers currently use PHRs and fifty-seven percent were "not at all interested" in accessing PHRs online).

87. IMS Health Inc. v. Ayotte, 490 F. Supp. 2d 163, 167 (D.N.H. 2007), *rev'd*, No. 07-1945, 2008 WL 4911262 (1st Cir. Nov. 18, 2008).

88. United States Dep't of Health & Human Servs., Off. of National Coordinator: Mission, http://www.hhs.gov/healthit/onc/mission (last visited May 17, 2009).

> have rigid restrictions on, for example, the secondary use of data by some kinds of PHR vendors but not others.[89]

If the PHR data remains in its patient-controlled silo and is never shared, PCS legal issues will seldom arise. But, as soon as the patient shares the data, very different legal regimes may apply to that data going forward. Thus, a single piece of data may have very different PCS legal properties depending on whether it is exported to (shared with) a HIPAA-regulated provider or a different kind of third party such as a health information web site, or again if it is shared back (re-imported) to the patient-maintained PHR.[90]

C. Deficiencies in Legal PCS Models

Our current legal model for protecting medical information rotates around regulatory requirements for confidentiality and security. Confidentiality rules limit access to previously disclosed patient data, while security requirements provide the correlate, seeking to restrict unauthorized access to those not within the circle of confidence. This model generally eschews privacy requirements in that it tends not to place any restrictions on the *collection* of medical data.

The deficiencies with our legal confidentiality and security models primarily lie in their execution. As described elsewhere, the federal HIPAA confidentiality code rules (mislabeled as protective of "privacy") are conceptually and operationally defective. First, rather than clearly establishing the

---

89. ALTARUM, INC., REVIEW OF THE PERSONAL HEALTH RECORD (PHR) SERVICE PROVIDER MARKET, PRIVACY AND SECURITY 14 (2007), *available at* http://www.hhs.gov/healthit/ahic/materials/ 01_07/ce/PrivacyReview.pdf [hereinafter *2007 ONCHIT Study*] (report prepared by ALTARUM, Inc. for ONCHIT).

90. This state of affairs seems to be recognized by the Google Health privacy policy:

> Some of these third-party websites will be covered by federal and state health privacy laws (such as the Health Insurance Portability and Accountability Act, or "HIPAA"), and those laws will govern how they may use and share your information. As a result, you must authorize these providers to send information to your Google Health account. With that authorization, you also give them permission to send certain types of health information (such as mental health records) that are protected by federal and state laws and require special authorization. When you ask Google to send your health information to others, you will also be giving Google permission to send those certain types of health information.

Google Health, Google Health Privacy Policy, http://www.google.com/health/html/privacy.html (last visited May 17, 2009).

principle of confidentiality and patient rights, the regulation concentrates on exceptionalism—cataloging the *process* of patient consent to disclosure. Second, these recognized exceptions are quite broad, permitting disclosure of patient data to public health, judicial, and regulatory interests that likely would exceed patient expectations.[91] Third, in an environment where so many "outsiders" such as pharmaceutical companies and data aggregators covet medical data, the regulatory standards have only limited protections against the use of patient data outside of treatment and billing. Fourth, there are considerable concerns about the enforcement of the regulations even as they stand.[92] Fifth, it is an understatement to say that the confidentiality code lacks transparency or clarity and that it fails to send any principled or educational "message" to patients as to their data rights.[93] Sixth, considerable doubts have been raised as to the level of the federal government's commitment to the enforcement of the HIPAA rules.[94]

Of all the general criticisms that can be leveled at the federal confidentiality code, however, there is one that is particularly glaring in the context of PHRs. There are serious gaps in the regulations (a function of limitations in the enabling legislation) that will result in HIPAA protections not reaching data held in most PHRs. Truly, most PHRs will exist in a PCS regulation-free zone because the "privacy" (confidentiality) and security rules apply only to health plans, health care clearinghouses, or health care providers[95] who engage in HIPAA electronic transactions.[96] As a result, non-traditional custodians of medical data will not be subject to the regulations.[97] Some

---

91. 45 C.F.R. § 164.512 (2007); *see also* Kalinoski v. Evans, 377 F. Supp. 2d 136, 139 (D.D.C. 2005) (citing § 164.512).

92. There is also generalized laxness, as HIPAA compliance declines. *See* Nancy Ferris, *Privacy Rule Compliance Said to Be Diminishing*, GOVERNMENT HEALTH IT, Apr. 19, 2006, http://www.govhealthit.com/online/news/94120-1.html.

93. *Ensuring Privacy*, *supra* note 12, at 713-17; *see also What's Wrong with Health Privacy*, *supra* note 79.

94. *See, e.g.*, Rob Stein, *Medical Privacy Law Nets No Fines, Lax Enforcement Puts Patients' Files at Risk, Critics Say*, WASH. POST, June 5, 2006, at A01.

95. 45 C.F.R. §§ 160.103, 164.502 (2007).

96. 45 C.F.R. § 164.104 (2007). For an explanation of HIPAA transactions, see Nicolas P. Terry, *An eHealth Diptych: The Impact of Privacy Regulation on Medical Error and Malpractice Litigation*, 27 AM. J.L. & MED. 361, 365-66 (2001).

97. *See* Beard v. City of Chicago, No. 03 C 3527, 2005 WL 66074, at *2 (N.D. Ill. Jan. 10, 2005) (holding city fire department is not a covered entity under HIPAA); *see also* United

PHRs may be included; for example, PHRs provided by doctors, hospitals, or health plans generally will be swept into the HIPAA ambit. Further, some "branded" PHRs supplied by third parties at the behest of covered entities may be subject to the "business associate" extension.[98] However, PHRs supplied by employers, non-health (e.g., life) insurers, and third party, web-based PHRs generally will avoid HIPAA regulation.[99]

If the federal regulations are inapplicable, will state laws protect PHR data? The HIPAA confidentiality code does not preempt "more stringent" state law,[100] and most states have some form of PCS legislation that protects medical information against disclosure.[101] Although state law is not hidebound by the limitations of HIPAA applicability, few are sufficiently comprehensive to include PHRs.[102]

At the very least PHRs engender complex legal indeterminacies as to the application of federal and state protections. Potentially, PHR suppliers will be able to exploit their HIPAA-free space and externalize many of the PCS risks inherent in their products and services to patients. A 2007 study prepared for ONCHIT posed the following questions:

> • Should the consumer be informed every time there is any secondary use of the data, for example sale of aggregated data to a pharmacy benefits manager for utilization review?

States v. Mathis, 377 F. Supp. 2d 640, 645 (M.D. Tenn. 2005) (holding FBI not a covered entity).

98. *See* 45 C.F.R. §§ 160.103, 164.504(e) (2007).

99. *See generally* Assoc. Press, *Google Online Health Records Service Irks Privacy Watchdogs*, FOX NEWS, May 20, 2008, http://www.foxnews.com/story/0,2933,356663,00.html (stating that Google Health and similar services are not covered by HIPAA). In this context, 45 C.F.R. § 160.103 (2007) may apply to exclude employers who are otherwise covered entities if the data is viewed as contained in employment records.

100. 45 C.F.R. §§ 160.202-160.203 (2007).

101. Of course most states also recognize the common law action for breach of confidence. *See generally Ensuring Privacy*, *supra* note 12, at 712-13 (discussing torts-based cause of action for breach of confidence under common law).

102. California and Washington State have exceptional protections. *See* CAL. CIV. CODE § 1798.81.5 (West Supp. 2008) (including medical information as protected personal information under state law. Medical information is defined as "any individually identifiable information, in *electronic* or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional." (emphasis added). This definition is sufficiently comprehensive to include PHRs.); WASH. REV. CODE ANN. §§ 19.215.010, 19.215.020 (West 2007) (including information that "relates to medical history or status" in the definition of "personal financial" and "health information." Also, providing for a civil action for careless disposal of such information.).

> • Should all current third-party users of de-identified or individually identifiable data be explicitly named by the PHR vendor?
>
> • Should the consumer be required to explicitly opt-in prior to any transfer or sale of individually identifiable PHR data?
>
> • Should the vendor be required to notify all consumers of any change in privacy policy? Should a written copy of the privacy policy be mailed to every PHR customer on a periodic basis, as is required for consumer credit?
>
> • Should vendors be required to notify all affected consumers in the event of an accidental privacy breach? What if that breach takes place in a business partner, an Application Service Provider (ASP) vendor, or other third party? Must the data involved in the breach be provided to consumers affected?
>
> • Should a history of the vendor's privacy breaches, accidental disclosures, or other unauthorized access or viewing of PHR data be provided to all PHR consumers, perhaps on demand?
>
> • Should a seal of approval or other privacy certification or audit of privacy policies be developed, and provided by a non-profit consortium, government agency, or for-profit firm?
>
> . . . .
>
> • Should all vendors be required to be able to document their chain-of-custody process for all PHR data they may hold, perhaps for audit or other investigatory purposes?
>
> • Should all PHR vendors be covered under HIPAA?[103]

In the next section, I examine potential legal vehicles with which to address some of these difficult questions.

---

103. *2007 ONCHIT Study*, *supra* note 89, at 16.

V. ADDRESSING THE PHR PRIVACY-CONFIDENTIALITY-SECURITY ISSUES

Given the limited applicability of traditional PCS legal protections to PHRs, is it possible to harness some less well-known or even less formally legalistic approaches? This section critically examines some potential alternatives such as security breach notification, privacy policies, and voluntary compliance with HIPAA. With seeming inevitability it concludes by once again addressing the reform of HIPAA itself.

A. Breach Notification Statutes

The HIPAA security rule while imposing related duties such as system audits[104] does not require notification of breach. Some state codes (apparent Security Rule preemption notwithstanding[105]) do impose medical records-specific requirements as to recording information disclosures.[106]

Primarily aimed at financial identity theft, a security breach notification law is a relatively new construct that has joined the PCS legal constellation. California passed the first such statute, which became effective in July 2003.[107] More than forty states now have some type of breach notification statute.[108] There are many flavors of this type of legislation with different advantages and disadvantages.[109] The basic model, however, is to create some threshold (e.g., a reasonable belief in the data custodian that the data has been acquired by a third party or, alternatively, a reasonable belief that it has been acquired *and*

104. *See* 45 C.F.R. § 164.312(b) (2007).

105. *See* 68 Fed. Reg. 8334, 8362 (Feb. 20, 2003) (codified at 45 C.F.R. pt. 160) (discussing preemption).

106. *See, e.g.*, FLA. STAT. ANN. § 456.057(12) (West 2007) ("Records owners are responsible for maintaining a record of all disclosures of information contained in the medical record to a third party, including the purpose of the disclosure request. The record of disclosure may be maintained in the medical record. The third party to whom information is disclosed is prohibited from further disclosing any information in the medical record without the expressed written consent of the patient or the patient's legal representative.").

107. CAL. CIV. CODE § 1798.82 (West Supp. 2009).

108. Nat'l Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited May 17, 2009).

109. Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915-18 (2007) (discussing and distinguishing "the different aspects of breach notification and identify[ing] trade-offs that arise when a notification approach emphasizes one or another").

misused) that triggers a duty to notify the consumer and, in some jurisdictions, other interested parties such as consumer protection agencies or credit reporting agencies (frequently also triggering a security "freeze" on the consumer's file).[110] Not surprisingly, this explosion of diverse state provisions affecting nationwide data custodians has led to calls for a federal, preemptive measure. For example, the Identity Theft Prevention Act[111] would require data custodians to have written security programs and notify the Federal Trade Commission (FTC), credit-reporting agencies, and affected individuals of security breaches involving "sensitive personal information," and facilitate freezes on credit reports. At the beginning of 2008 there were nine, often conflicting bills before the 110th Congress, bottled up in various House and Senate committees.[112]

Thefts of medical identity represent only three percent of identity theft but there are concerns that it is on the rise.[113] A review of the state breach statutes shows considerable inconsistency regarding the treatment of medical data breaches. There are at least three extant models. In the first model, state breach notification statutes, while not explicitly excluding medical data, appear not to be applicable because of the relatively narrow types of data they protect (such as driver's license and social security numbers and financial information).[114] This is also the case with the federal initiatives. For

110. *See, e.g.*, LA. REV. STAT. ANN. § 9:3571.1(H)(4)-(5) (Supp. 2008) (consumer may request "freeze" in case of identity theft); H.B. 2245, 51st Leg., 2d Reg. Sess. §3(C) (Okla. 2008) (consumer shall be notified "as soon as practicable following discovery, if the personal information was or if the entity reasonably believes was accessed and acquired by an unauthorized person").

111. Identity Theft Prevention Act, S. 1178, 110th Cong. (2007).

112. Alexei Alexis, *Outlook 2008: Data Security, Murky Outlook Seen for Federal Date Breach Notification Legislation in 2008*, PRIVACY LAW WATCH (BNA), Jan. 17, 2008, http://www.bna.com/products/ip/pwdm.htm (sign in to subscription service; then search "Murky Outlook Seen for Federal Date Breach Notification Legislation in 2008").

113. Michelle Andrews, *Medical Identity Theft Turns Patients Into Victims*, U.S. NEWS & WORLD REPORT, Feb. 29, 2008, http://health.usnews.com/articles/health/living-well-usn/2008/02/29/medical-identity-theft-turns-patients-into-victims.html.

114. *See, e.g.*, COLO. REV. STAT. ANN. § 6-1-716 (West Supp. 2008); CONN. GEN STAT. ANN. § 36a-701(b) (West Supp. 2008); DEL. CODE ANN. tit. 6, §§ 12B-101 to -104 (2005); FLA. STAT. ANN. § 817.5681 (West 2006); GA. CODE ANN. §§ 10-1-911 to -912 (West Supp. 2008); IDAHO CODE ANN. §§ 28-51-104 to -107 (2008); 815 ILL. COMP. STAT. ANN. §§ 530/5, /10, /12, /20 (West 2008); IND. CODE ANN. §§ 24-4.9-2-10, 24-4.9-3-1 to -4, 24-4.9-4-1 to -2 (LexisNexis 2006 & Supp. 2008); KAN. STAT. ANN. §§ 50-7a01 to-7a02 (Supp. 2006); ME. REV. STAT. ANN. tit. 10, §§ 1347-49 (Supp. 2008); MINN. STAT. ANN. § 325E.61 (West Supp. 2008); MONT. CODE ANN. § 30-14-

example, the Identity Theft Prevention Act definition of "sensitive personal information" does not extend to medical data.[115] The second model is to explicitly include medical information or health insurance data, thus extending breach notifications to cases of medical identity theft but to exclude custodians who are HIPAA "covered entities."[116] A third model applies the state statute generally to medical information, but excludes data custodians subject to *and in compliance with* HIPAA.[117]

Unsurprisingly, given its subject matter, but unlike most state or proposed federal breach notification laws, the TRUST in Health Information Act of 2008[118] would have required medical data stewards or processors to notify individuals of security breaches. Therein, a "health information person," defined sufficiently broadly so as to include most PHR service providers,[119] would have been under a duty to notify individuals of security breaches involving personal health information within fifteen days of the discovery of the breach.[120] The HITECH Act of 2009, passed as a part of the stimulus bill adds its own version of a breach notification provision, as discussed below.[121]

1704 (2007); N.Y. GEN. BUS. LAW § 899-aa (Consol. Supp. 2008); OHIO REV. CODE ANN. §§ 1347.12, 1349.19, 1349.191-.192 (LexisNexis 2006 & Supp. 2008); TEX. BUS. & COM. CODE ANN. §§ 48.002, .103, .201 (Vernon Supp. 2008); UTAH CODE ANN. §§ 13-44-102, -201, -202, -301 (Supp. 2008).

115. S. 1178.

116. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501(J)(2) (Supp. 2008); CAL. CIV. CODE § 1798.81.5e)(3) (West Supp. 2008); *see also* MD. CODE ANN., COM. LAW § 14-3501 (LexisNexis Supp. 2008) (which seems limited in its scope so as to apply to financial information and identifiers, § 14-3501(d)(1), but explicitly excludes "Information that is disseminated or listed in accordance with the [HIPAA]." § 14-3501(d)(2)(iii). Presumably this would therefore exclude financial information contained in HIPAA records.).

117. *See, e.g.*, HAW. REV. STAT. § 487N-2(g)(2) (Supp. 2007), *amended by* S.B. 2402, 24th Leg., Reg. Sess. (Haw. 2008) (deeming a business in compliance with the notification statute if it is "Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information of [HIPAA]."); *see also* MICH. COMP. LAWS ANN. § 445.72(10) (West Supp. 2008) (deeming compliance with breach notification statute if a "person or agency . . . is subject to and complies with the [HIPAA] . . . for the prevention of unauthorized access to customer information and customer notice"); S.B. 583, 74th Or. Leg. Assem., Reg. Sess. (Or. 2007) (deeming compliance with breach notification statute if a "person . . . is subject to and complies with regulations implementing the [HIPAA]").

118. TRUST in Health Information Act of 2008, H.R. 5442, 110th Cong. (2008).

119. *Id.* § 171(13).

120. *Id.* § 113.

121. *See infra* notes 194-207 and accompanying text.

Assume, therefore, that a comprehensive breach notification duty was imposed on PHR data custodians. What would be its value? Credit reporting freezes and records corrections duties may reduce the impact of financial identity theft, but would notification to a patient that his medical data has been compromised have a similar ameliorative effect? In the medical records context there seems to be only indirect value (such as identifying a PCS defendant) in telling the patient that the barn door has been open and the horse has bolted.

B. Privacy Policies

As I have argued elsewhere, non-governmental regulatory models for health care-related web services, such as codes of conduct and privacy policies, have had a generally unsatisfactory history.[122] Even assuming that they were beneficial (or even read by consumers[123]), however, Internet privacy policies have little relevance to the PHR security, confidentiality, and privacy issues discussed herein.[124] Privacy models and policies promulgated by well-known organizations such as TRUSTe[125] are aimed at ancillary data collection and processing by web sites that request personal information or use tracking cookies or GIF "Bugs." While PHR web applications

---

122. 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. OF HEALTH POL'Y L. & ETHICS 183, 239-46 (2004); Nicolas P. Terry, *Rating the 'Raters': Legal Exposure of Trustmark Authorities in the Context of Consumer Health Informatics*, 2 J. MED. INTERNET RES. e18 (2000), *available at* http://www.jmir.org/2000/3/e18/HTML.

123. Press Release, TRUSTe, Consumers Have False Sense of Security About Online Privacy–Actions Inconsistent with Attitudes (Dec. 6, 2006), http://www.truste.org/about/press_release/12_06_06.php (noting that, of the consumers who provide personal information to a web site for the first time, 72% failed to check "most of the time" whether the site has a privacy policy, and that 80% failed to read the policy if provided).

124. *See also 2007 ONCHIT Study*, *supra* note 89, at 10 ("There appears to be some confusion here by vendors, who describe Internet privacy policies for information collected by interaction with the Web site (cookies, Web logs) rather than privacy policies for the PHR data, however collected.").

125. The TRUSTe Home Page, suggests privacy policy language, inspects sites prior to authorizing them to use its trustmark, and provides some dispute resolution services. TRUSTe does not mandate the specifics of a privacy policy (e.g., any requirement that the site not share data with others), but rather suggests various alternative statements. *See generally* TRUSTE, GUIDANCE ON MODEL WEB SITE DISCLOSURES 2-9, http://www.truste.org/docs/Model_Privacy_Policy_Disclosures.doc (last visited May 17, 2009) (for example, "We share aggregated demographic information about our user base with our partners and advertisers. This information does not identify individual users.").

may not be immune from this kind of surreptitious data acquisition, the core purpose of the PHR business relationship is the storage and processing of the patient's identifiable health information. Most existing privacy policy models are therefore irrelevant or of limited value.

So, what would an industrial strength PHR privacy policy require? A 2007 ONCHIT study of the privacy policies of thirty PHRs constructed a baseline of thirty-one areas that a PHR privacy policy should address, from issues such as readability (what would happen to the data if the vendor went out of business) to data gathering and sharing.[126] The study found that ninety-seven percent of the policies surveyed addressed fifteen or fewer of those issues.[127] As an example, only one of the thirty privacy policies included a statement that explicit patient consent was necessary prior to the vendor sharing data stored in a PHR.[128]

The fatal flaw of the privacy policy model is that web sites can avoid legal jeopardy by not posting a policy, or using one that is so rudimentary that it provides no real protection for users. While several states have enacted a privacy policy[129] and other privacy protections[130] for their own official sites, very few jurisdictions have addressed the question of commercial web sites.[131] Indeed, only California has anything more than a rudimentary model, requiring web sites to "conspicuously post [a] privacy policy,"[132] that identifies "the categories of personally identifiable information that the operator collects and the categories of third-party persons or entities with whom the operator may share that personally identifiable information."[133] It is this California law that has engaged the

126. *2007 ONCHIT Study*, *supra* note 89, at 4-13.

127. *Id.* at 6.

128. *Id.* at 7.

129. *See, e.g.*, S.C. CODE ANN. § 30-2-40 (2007) (requiring privacy policy).

130. *See, e.g.*, 5 ILL. COMP. STAT. 177/10 (2008) (prohibiting tracking cookies).

131. *See, e.g.*, NEB. REV. STAT. § 87-302(a)(14) (2006) (making it a deceptive trade practice to knowingly make "a false or misleading statement in a privacy policy, published on the Internet"); 18 PA. CONS. STAT. § 4107(a)(10) (2008) (making it a deceptive or fraudulent business practice to knowingly make "a false or misleading statement in a privacy policy, published on the Internet").

132. CAL BUS. & PROF. CODE § 22575(a) (West 2008).

133. *Id.* at § 22575(b)(1). "Personally identifiable information" is defined to include "[i]nformation concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier…." *Id.* §

blogosphere in a debate about whether Google was in compliance when it refused to link its privacy policy from its traditionally "clean" front page;[134] a question that has added importance given Google's entrance into the PHR market. The TRUST in Health Information Act of 2008 would require a "health information person" such as a PHR provider to publish a written privacy policy.[135] This policy would have to include a detailed description of the data subject's rights including various consent and opt-out rights.

Assume, however, that a web site does post a more granular privacy policy that addresses issues specific to PHR data. What is the legal effect? For example, Google Health states:

> 1. You control who can access your personal health information. By default, you are the only user who can view and edit your information. If you choose to, you can share your information with others.
>
> 2. Google will not sell, rent, or share your information (identified or de-identified) without your explicit consent, except in the limited situations described in the Google Privacy Policy, such as when Google believes it is required to do so by law.[136]

Another web vendor addresses specifically the question of the patient-employees data privacy vis-à-vis a sponsoring employer: "If your . . . service is provided by your employer, that employer acts as a sponsor. Under no circumstances will your confidential medical data be made accessible or sold to your employer."[137]

In either case, the breach of such a policy could trigger contractual remedies, while the policy language likely would feed the expectations upon which a patient could build a breach of

---

22577(a)(7).

134. Posting of Saul Hansell to Bits, *Is Google Violating a California Privacy Law?*, http://bits.blogs.nytimes.com/2008/05/30/is-google-violating-a-california-privacy-law/ (May 30, 2008, 08:45 EST). On July 3, 2008, Google added such a link. *See* Posting of Saul Hansell to Bits, *Google Changes Home Page, Adding Link to Privacy Policy*, http://bits.blogs.nytimes.com/ (Search for "California Privacy Law") (July 4, 2008, 10:07 EST).

135. TRUST in Health Information Act of 2008, H.R. 5442, 110th Cong. § 111 (2008).

136. Google Health Privacy Policy, http://www.google.com/health/html/privacy.html (last visited Dec. 16, 2008).

137. Securamed, Frequently Asked Questions, http://www.securamed.com/support_english.med (last visited Dec. 16, 2008) ("What role does my employer play?").

confidence action. More importantly, the PHR provider would be subject to action by consumer protection agencies such as the FTC.[138] Under the TRUST in Health Information Act of 2008, breach of the requirement of a privacy policy or of a required data subject right contained therein could lead to federal civil penalties, private actions, or state attorney general enforcement.[139]

The ONCHIT study suggested several important features for any PHR privacy policy, including "complete transparency on the release of PHR data to any third-party," disclosure of "all business relationships relating to the handling, processing, data mining, or other management of PHR data," and descriptions of "the relationship of the vendor's policies to HIPAA requirements . . . and other relevant Federal rules and regulations."[140] Not surprisingly, given that the Achilles' heel of the PHR construct is its inchoate interoperability with third parties (whether by import or export of data), one of the fundamental flaws in current privacy policies concerns third party relationships. Again, take the Google Health policy regarding data that a patient shares with a third party, Google partner:

> 2. Google Health contains a directory of third-party websites that are capable of securely sending information to Google Health. These websites (which may include your medical provider) may give more information about certain conditions or extend the functionality of Google Health in other ways. By creating a link to these websites, you give them permission to send you information such as medical records, prescription histories, or test reports.
>
> 3. You can approve access for some of these websites to view your health information. If a website accesses

138. *See generally* Fed. Trade Comm'n, Enforcing Privacy Promises: Section 5 of the FTC Act, http://www.ftc.gov/privacy/privacyinitiatives/promises.html (last visited May 17, 2009) (discussing Commission's practice of enforcing privacy policies and challenging company practices that cause substantial consumer injury); Complaint and Request for Injunction, Request for Investigation and for Other Relief Before the Federal Trade Commission, In re Ask.com, filed Jan. 19, 2008, *available at* http://epic.org/privacy/ask/epic_askeraser_011908.pdf (arguing that defendant's representations as to the persistence of personal data when using their web search service "AskEraser" constitute deceptive and misleading practice).

139. H.R. 5442 §§ 151-52.

140. *2007 ONCHIT Study*, *supra* note 89, at 15.

> your health information and stores a copy of your information, that copy will be governed by that website's privacy policy. Others at that facility–like an on-call doctor–may be able to view your information. Google is not responsible for the content, performance, or privacy policies of third-party websites.
>
> . . . .
>
> 5. All third-party websites listed in the directory are contractually required to abide by the Google Health Developer Policies, which establish strict privacy standards for how they collect, use, or share your information.[141]

This welcome transparency from a leading and well-respected internet provider poses more questions than it answers. Clearly, most partners of a PHR provider will have compelling commercial incentives to comply with the privacy policies contained in a development agreement. However, even leaving aside any privity questions, this contractual construct falls short of even the often-criticized HIPAA "Business associate" extension.[142]

Overall, however, the privacy policy approach to dealing with PHR PCS issues is at best immature. In the absence of the PHR vendors agreeing to a granular, standardized privacy policy (including but not limited to voluntary compliance with HIPAA standards) the approach will remain incoherent.

C. HIPAA as Guideline?

Closely related (functionally and legally) to increased use of privacy policies is the proposal that PHR vendors voluntarily comply with HIPAA. The ONCHIT study of PHR privacy policies found that only twenty-six percent of vendors even referenced HIPAA standards.[143] The study's authors noted:

> We would have expected more vendors to at least reference HIPAA . . . . Since the legal landscape is so un-

141. Google Health Privacy Policy, *supra* note 135.

142. 45 C.F.R. § 164.504(e). *Cf.* H.R. 5442 § 114(a)-(b) (providing for enhanced transparency regarding data partners).

143. *2007 ONCHIT Study*, *supra* note 89, at 12.

> clear on the privacy requirements of PHR service providers, it would make sense that many of them would use HIPAA as a guideline in formulating their policies. In addition there could be significant marketing advantages from referencing HIPAA, as many users, providers and payers are familiar with it.[144]

Leaving aside the doubtful assertion that "many users" are familiar with the intricacies of the HIPAA PCS construct and the many flaws in HIPAA already discussed,[145] what would voluntary compliance with HIPAA provisions do to further PHR PCS? Certainly, co-opting the Administrative,[146] Physical,[147] and Technical Safeguards[148] contained within the Security Rule would be positive. However, the terrain is less certain with regard to confidentiality. Distilled to a single principle (not an easy task) the HIPAA code requires health care providers to limit unauthorized disclosures of patient information to those involved in health care and billing. Yet, that presupposes a fundamentally different relationship from the one between a patient and a PHR provider.

The HIPAA rules assume that the regulated entities, some "Business associates"[149] aside, are health care providers. For example, providers have been told that the discretion inherent in many of HIPAA's "permitted uses"[150] is to be exercised with "professional ethics and best judgment."[151] Further, for several of its rules the HIPAA code assumes that the data custodian can differentiate between ordinary medical records and "Psychotherapy notes."[152]

---

144. *Id.*

145. *See supra* notes 91-99 and accompanying text.

146. 45 C.F.R. § 164.308 (2007).

147. *Id.* § 164.310.

148. *Id.* § 164.312.

149. *See, e.g.*, 45 C.F.R. § 160.103 (2007) (defining "Business associate"); 45 C.F.R. § 164.502(e) (2007) (disclosures to business associates), 45 C.F.R. § 164.504(e) (2007) (business associate contracts); 45 C.F.R. § 164.532(d) (2007) (effect of prior contracts or other arrangements with business associates).

150. *See, e.g.*, 45 C.F.R. §§ 164.512, 164.514 (2007).

151. OFFICE OF CIVIL RIGHTS, UNITED STATES DEP'T OF HEALTH AND HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 4-5 (2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. Nothing here suggests that the better PHR providers do not have ethics or best judgment, but these are derived from quite different core IT competencies and processes.

152. *See* 45 C.F.R. § 164.501 (2007) (defining "Psychotherapy notes"), 45 C.F.R. §

Several other points of disconnection can be observed. Take just one: HIPAA permits unfettered use of de-identified data.[153] It is at least arguable that patients do not object to health care providers sharing de-identified data as a public good, but their altruism may not extend to PHR vendors, whom they are directly paying to store their records, when they seek to monetize them.

This disconnect continues in the area of enforcement. HIPAA lacks a private right of action and its enforcement powers are vested in a regulatory office within the Department of Health and Human Services's (DHHS) Office of Civil Rights (OCR) that specializes in dealing with traditional health care entities.[154] If OCR were to investigate a PCS claim and find a breach by a PHR vendor what would be the remedy? Even if vendors voluntarily complied with HIPAA requirements how could that open them up to civil money[155] or criminal penalties[156] under a statute that on its face does not include them?

If an external normative structure is suggested as the basis for voluntary compliance, it might be preferable to look at some of the state statutory medical privacy models. For example, California's Confidentiality of Medical Information Act,[157] while based on a premise similar to HIPAA's (confidentiality of medical information collected by health care providers[158]), is unencumbered by many of the limitations of applicability in the HIPAA statute and extends to:

> [a]ny business organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the indi-

164.508(a)(2) (2007) (stating generally "a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes").

153. *See, e.g.*, 45 C.F.R. §§ 164.502(d)(2), 164.514(a)-(b).

154. *See* United States Dep't of Health & Human Servs., Office for Civil Rights, http://www.hhs. gov/ocr/office/index.html (last visited May 17, 2009).

155. 42 U.S.C. §1320d-5 (2007).

156. 42 U.S.C. §1320d-6 (2007).

157. Confidentiality of Medical Information Act, CAL. CIV. CODE §§ 56.07-.37 (Deering 2007).

158. *Id.* § 56 note.

vidual to manage his or her information.[159]

The substantive provisions, while suffering from some of the same assumptions that the data custodian is typically a health care provider, provide for more robust confidentiality protections[160] and require a "contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall do so in a manner that preserves the confidentiality of the information contained therein."[161] Any such contractor "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records"[162] is subject to administrative and criminal penalties,[163] and a private right of action by the patient.[164]

D. Reforming HIPAA

The limitations inherent in notification of breach statutes, privacy policies, and voluntary compliance with HIPAA, coupled with a need for national standards applicable to something like border-agnostic web data, leads the discussion back to a relatively unpalatable imperative–statutory reform of the HIPAA code.

This is unpalatable because there is so little political will to reopen the federal standards.[165] Lack of Congressional agreement led to the development of the HIPAA transactional, privacy, and security standards being handed off to DHHS. Providers intensely dislike HIPAA protections, and privacy advocates may be loath to reopen the discussion lest the fragile protections of HIPAA are watered down. A "simple fix" to the HIPAA PCS regulations, to extend their provisions to PHR providers, would have the same flaws identified above in dis-

159. *Id.* § 56.06(a).

160. *Id.* § 56.10.

161. *Id.* § 56.101.

162. *Id.*

163. *Id.* § 56.36.

164. *Id.* §§ 56.35-.36.

165. *Cf. House Speaker Calls for EHRs in 2008 Health Policy Proposals*, iHEALTHBEAT, Jan. 28, 2008, http://www.ihealthbeat.org/articles/2008/1/28/House-Speaker-Calls-for-EHRs-in-2008-Health-Policy-Proposals.aspx?topicID=54 (quoting Speaker Pelosi, speaking in favor of EHRs at a conference in January 2008, as saying "Essential to [improving health care through EHRs], though, is protecting confidentiality and privacy. If we have the technology or if we don't, we must [ask] for the technology to make that possible.").

cussing voluntary compliance.[166] A lower-key solution, federal legislation aimed specifically at PHRs, would be next to impossible to harmonize with the existing confidentiality code because of the overlaps between provider records and PHRs.

Yet, what is the alternative? States are increasingly comfortable in once again legislating on medical data confidentiality (in part because of HIPPA's "more stringent" limitation on preemption) and identity theft issues. A heterogeneous patchwork of state protections will return us to pre-HIPAA times and dramatically increase barriers to crucial HIT initiatives. Indeed, this disconnect is at the core of the electronics records PCS debate. One of the original impediments to a national EHR identified by the Bush Administration was lack of uniformity requiring ONCHIT to, in the words of Dr. Brailer, "[address] variations in privacy and security policies that can hinder interoperability."[167] Advocates of the national EHR translated this into replacing the HIPAA "floor," whereby more stringent state privacy protections are not preempted,[168] with a HIPAA "ceiling," tipping the balance away from patient PCS protections in order to facilitate the national EHR.[169]

In a prior article, Leslie Francis and I took the opposite approach, calling for specific PCS-enhancing reforms to take into account general deficiencies in the federal legal model and to respond to the PCS challenges inherent in a national, interoperable EHR program. While supportive of a HIPAA ceiling we advocated reforming HIPAA to considerably increase pa-

166. *See supra* note 143 and accompanying text.

167. *Activities of the Office of the National Coordinator for Health Information Technology: Testimony before the S. Comm. on Commerce, Science, and Transportation Subcomm. on Technology, Innovation, and Competitiveness*, 109th Cong. (2005) (statement of David J. Brailer, M.D., Ph.D., National Coordinator for Health Information Technology, U.S. Department of Health and Human Services), *available at* http://www.hhs.gov/asl/testify/t050630a.html [hereinafter *Brailer Testimony*].

168. 45 C.F.R. §§ 160.202-.203 (2007).

169. *See, e.g.*, BRUCE MERLIN FRIED, CALIFORNIA HEALTHCARE FOUNDATION, GAUGING THE PROGRESS OF THE NATIONAL HEALTH INFORMATION TECHNOLOGY INITIATIVE: PERSPECTIVES FROM THE FIELD 12 (2008), *available at* http://www.chcf.org/documents/chronicdisease/GaugingTheProgressOfTheNationalHITInitiative.pdf [hereinafter GAUGING THE PROGRESS] (quoting Jeffrey Kang, M.D., chief medical officer for Cigna, on providing a chronology of the Nationwide Health Information Structure: "Typically, [the federal authorities] set a minimum and then states can go higher. On this one, in order for the free flow of information to improve quality, you actually want to set a maximum which states can't go above because you want to be able to guarantee some level of free flow.").

tient PCS protections.[170] These same reforms should be extended to PHR models. Thus, some types of data (for example prescription data) should be protected against even consented-to collection or disclosure to commercial entities; health care information should reside only in the medical domain; and an independent regulatory body should be appointed that will have the power to review the manner in which patient information is managed, to create codes of conduct, and to resolve disputes. At the very least, the limitations on HIPAA applicability must be removed. The last vestiges of HHS's "insider baseball" model, whereby HIPAA protections apply only to traditional healthcare providers and their close business partners, must be shed and replaced by a general federal medical privacy code that does not turn on provider minutiae, but focuses on the data itself.

Taking an approach that is perhaps attuned to the current political and legislative realities that apply to the data protection debate, the National Committee on Vital and Health Statistics (NCVHS)[171] in its *Stewardship Framework*[172] report, suggested tweaks to the HIPAA model, calling for stronger guidance, strengthening of business agreements and their parties' expectations, and calling on the FTC to increase its footprint in non-HIPAA regulated areas (such as PHRs). However, NCVHS also recommended:

> HHS should work with other federal agencies and the Congress . . . *for more inclusive, federal privacy legislation* so that all individuals and organizations that use and disclose individually identifiable health information are covered by the data stewardship principles inherent in such legislation, including a range of organizations not currently covered by HIPAA.[173]

In Europe, the Data Directive provides a data protection model that imposes robust obligations on data stewards and

---

170. *Ensuring Privacy*, *supra* note 12, at 730-35.

171. Nat'l Comm. on Vital and Health Statistics, http://ncvhs.hhs. gov/ (last visited May 17, 2008).

172. NAT'L COMM. ON VITAL AND HEALTH STATISTICS, REPORT ON ENHANCED PROTECTIONS FOR USES OF HEALTH DATA: A STEWARDSHIP FRAMEWORK FOR "SECONDARY USES" OF ELECTRONICALLY COLLECTED AND TRANSMITTED HEALTH DATA 16 (2007), *available at* http://www.ncvhs.hhs.gov/071221lt.pdf.

173. *Id.* at 46.

"chain of trust" data processors.[174] The foundation of this model is a proportionality rule,[175] which applies equally to both the *collection* and the *disclosure* of data, and limits the re-processing of data for purposes incompatible with the original purpose of collection.

Such basic principles must be at the core of reformed data protection in the United States. Ensuring trust and meeting patient expectations must drive the legislative process. Trust must be earned by permitting patient opt-out or data sequestering, while expectations are consistent with relatively unimpeded use of data for point of care and continuum of care purposes. Patient acceptance of *some* secondary uses will be more likely secured with strict limitations on commercial uses. Between these extreme groupings, patient trust must be earned through transparency as they are informed about the projected uses of their data and its level of de-identification.[176]

E. The Stimulus Package Compromise

The American Recovery and Reinvestment Act of 2009 (or Stimulus Bill)[177] passed by Congress and signed into law by President Barack Obama in February 2009 includes $20 billion for health information technologies. The core of the HIT pack-

---

174. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 1995 O.J. (L 281) 31, 31-50 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

175. *Id*. at Ch. II, §1, Art. 6 (1)(c) ("adequate, relevant and not excessive").

176. Measured against these criteria, the proposed TRUST in Health Information Act of 2008, H.R. 5442, 110th Cong. (2008), is a disappointment. Although the reach of many of its proposed PCS provisions is broader than those under HIPAA the bill retains some of HIPAA's "insider baseball" approach. *See* H.R. 5442; HIPPA, *supra* note 14. Thus, although privacy policy publication (§ 111), breach notification (§ 113), and data transparency (§ 114) provisions apply equally to PHR providers (as "health information persons" as defined in § 171(13)) and traditional health care providers (§ 171(12)), this is not the case with regard to the reformulated *Subtitle C – Use and Disclosure of Personal Health Information* (§§ 121-44). *See* H.R. 5442. That subtitle applies strengthened PCS provisions differently dependent upon whether the data custodian is a health information person or a traditional provider. H.R. 5442. Notwithstanding, the bill does display a considerable advance over HIPAA or related state statutes, for example, in its approach to proportionality (§ 121(b)), tying data use to the purpose for which it was disclosed (§ 121(c)), and an opt-out for network sharing of personal health information (§ 121(k)). *See* H.R. 5442. Consent processes for treatment or payment (§ 122) and other uses (§ 123) are also strengthened. *See* H.R. 5442.

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

age is the stimulation of EMR adoption and the creation of regional or nationwide interoperability for such records;[178] the ONCHIT Coordinator being instructed to adopt a strategy leading to "[t]he utilization of an electronic health record for each person in the United States by 2014."[179]

The program includes funding for regional health information exchanges and involves the largest incentive payments to Medicaid and Medicare providers who adopt interoperable EMRs.[180]

Title XIII of the Stimulus Bill is the Health Information Technology for Economic and Clinical Health Act (HITECH).[181] HITECH provides the operational structure and regulatory authority for the HIT initiatives, such as governance, product certification, incentive programs, research, testing, and reporting. Of particular note is Subtitle D of HITECH, entitled "Privacy."[182] Subtitle D makes a number of changes in the regulation of health information generally and electronic health records in particular.

First, HITECH closes some of the regulatory gaps in HIPAA. Thus, "Business associates" are no longer indirectly regulated through terms in their contracts with "Covered Entities" but are directly subject to the HIPAA code,[183] including its penalties.[184] Second, HITECH seeks to respond to criticisms about HIPAA's lack of an educative goal, requiring regulations on educating health providers,[185] and an initiative to "enhance public transparency regarding the uses of protected health information."[186] Third, the new legislation requires new regulations tightening up the idea of proportionality ("minimum necessary" under HIPAA) in disclosures.[187] Fourth, there are new restrictions on the use of protected health information for

178. Kevin Freking, *Obama Team Sees Stimulus Advancing Health Reform*, GUARDIAN, Feb. 14, 2009, http://www.guardian.co.uk/worldlatest/story/0,,-8358685,00.html.

179. § 3001(c)(3)(A)(ii).

180. §§ 4101-02.

181. § 13001(a).

182. §§ 13400-24.

183. § 13401(a)-(b).

184. § 13404.

185. § 13403(a).

186. § 13403(b).

187. § 13405(b).

marketing purposes,[188] including a patient "opt-out" from fundraising communications.[189] Fifth, there are new, tighter definitions of breaches of the HIPAA code and provisions to improve enforcement,[190] including enforcement through state attorneys general.[191] Although there is still no private right of action, there will be a system designed to distribute a percentage of civil penalties or settlements collected from providers to injured patients.[192] In general, the HIPAA approach to preemption, the HIPAA "floor," continues.[193]

Going substantially beyond the original HIPAA model, HITECH adds a "breach notification" provision that applies to covered entities[194] and their business associates.[195] These provisions apply only to "unsecured protected health information,"[196] which, in the absence of further regulatory guidance,[197] means "protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute."[198]

Given that the focus of this section of the stimulus package was on promoting electronic health records by seeking to counter current market failures, it is perhaps surprising that HITECH contains little new regulation of privacy, confidentiality, or security that is specific to EHR data. The statute does include a definition of the EHR, although confusingly it is one that is generally associated with an EMR.[199] For the first time

188. § 13406(a).
189. § 13406(b).
190. §§ 13409-10.
191. § 13410(e).
192. § 13410(c)(3).
193. § 13421.
194. § 13402(a).
195. § 13402(b) (requiring business associate to notify the covered entity).
196. §§ 13402(a)-(b).
197. § 13402(h)(2).
198. § 13402(h)(1)(B).
199. *See* §13400(5) ("The term 'electronic health record' means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."). EHRs generally have been viewed as inherently interoperable. Presumably the new standards for EHRs will lead to all EMRs having that characteristic, thus rendering moot any distinction.

federal law now has a definition of a PHR: "The term 'personal health record' means an electronic record of PHR identifiable health information . . . on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[200]

Regarding EHR data, HITECH requires enhanced "accounting of disclosure" regulations[201] and regulations that generally will prohibit unconsented-to sale of EHR data.[202] Regarding PHRs, notably HITECH does not expand the definition of "covered entity" to include those who hold PHR data. Nevertheless, those who do so because of relationships with "covered entities" will be subject to the new tighter controls over disclosure and breach notification.[203] Instead PHR data stewards are subjected to a new "breach notification" provision. As with the general breach provisions,[204] this applies only to "unsecured" data.[205] Its reach is extended to a new species of "Business associate," known as a "third party service provider that provides services to a vendor of personal health records . . . ."[206]

Judgment as to the extent to which HITECH improves overall HIPAA protection of health data must be reserved (although not without some optimism) until the new regulations required to implement many, if not most, of its provisions are drafted and the implicit enforcement renaissance is translated into practice. Overall, however, and with the obvious exception of the breach notification provision (the efficacy of such a model having been doubted above[207]), PHRs remain in a relatively unregulated state, with most data risks still shifted to their data subjects.

VI. CONCLUSION

Technology is disruptive and tends to throw deficiencies in legal systems into sharp relief. Thus, the Bush Administra-

200. § 13400(11).
201. § 13405(c).
202. § 13405(d).
203. *See supra* notes 183-84 and accompanying text.
204. *See supra* notes 194-98 and accompanying text.
205. § 13407(a).
206. § 13407(b).
207. *See supra* Part V.A.

tion's commitment to a national interoperable health record put focus on the fact that HIPAA was not limited to insider financial transactions, but constituted the only national and somewhat deficient protection for patient data. The roll-out of PHR models continues this process. PHRs do much less than EHRs, yet their health quality implications and PCS risks are much greater.

The PHR narrative goes beyond innovation in e-health technologies and the development of new HIT business models. If PHRs gain traction we will have created a second, privatized channel of health care data that will lack the benefits of an EHR system (completeness, quality, universal availability, data-driven public health benefits, etc.). Whether or not PHRs reach critical mass, they illustrate the practical and legal problems we face when we shift risks away from providers and traditional payors to patients. PHRs, like the consumer-directed health care they enable, avoid many of the market failure issues that assault traditional health care models. Yet, their ascent introduces legal indeterminacies as to both records' quality and PCS protections.

The *existence* of PCS regulation is not such an impediment to EMR (or, by extension, health information technology) implementation that a PHR model enjoying a PCS regulation-free zone is a rational option. Physicians and patients will embrace both EMRs and PHRs when there is *more* not *less* PCS protection (and it will help if it is comprehensible). Any success enjoyed by PHRs will be muted once patients realize such medical information storage is not adequately protected by the legal system. EHRs and EMRs currently lack effective penetration primarily because of classic healthcare financing impediments. If, as seems likely, PHRs gain traction it will be because they appear not to be constrained by such impediments. However, that apparent advantage will be negated when patients realize that they now bear the costs and risks.

In the end, the success of *both* EHR and PHR models require fundamental reform of our privacy, confidentiality, and security approaches to medical information. Although it was not without flaws, the TRUST in Health Information Act of 2008[208] suggested that comprehensive reform was still possible. In

208. H.R. 5442.

early 2009, as the administration of President Obama began to tackle a worsening economic crisis, considerable investment in HIT was included in the initial federal stimulus package.

As the Obama Administration apparently has recognized, sophisticated HIT systems are key to reducing error, improving quality, and reducing our runaway health costs. But for those goals to be met, patients and providers must be willing, empowered, and protected participants.[209] The personal health record model, like its CDHC fellow traveler, must aspire to and deliver more than merely shifting additional risks to patients.

209. *See, e.g.*, GAUGING THE PROGRESS, *supra* note 168, at 12 ("It's not likely that state and federal policy on data flow can be harmonized without addressing issues of privacy. Lawmakers at all levels and the public at large oppose the loss of personal privacy. If this policy disconnect is to be addressed, a much broader public discussion must occur. Otherwise, clinicians and researchers will have difficulty gaining access to data they need to advance medical care.").