University of Baltimore Law Review

Volume 38
Issue 3 *Spring 2009*

Article 7

2009

Comments: Privacy at Risk: Patients Use New Web Products to Store and Share Personal Health Records

Juliana Bell
University of Baltimore School of Law

PRIVACY AT RISK: PATIENTS USE NEW WEB PRODUCTS TO STORE AND SHARE PERSONAL HEALTH RECORDS

I. INTRODUCTION

Physicians increasingly may begin their work days like Baltimore surgeon John Cameron, using computers to check patients' overnight test results before embarking to see the patients in person.[1] America is slowly shifting away from paper medical records,[2] including at Johns Hopkins Hospital in Baltimore where Cameron works.[3] One reason for the shift is that researchers believe electronic records may help reduce medical errors that kill up to 98,000 inpatients a year in U.S. hospitals.[4] Some doctors, for example, now "write" prescriptions via computer, avoiding the illegible handwriting that can lead pharmacists and nurses to accidentally give patients the wrong drugs.[5] The shift also promises efficiency as patients interact with their own hospital and clinic records by viewing them, scheduling appointments, or renewing prescriptions online.[6] Former President George W. Bush encouraged such efforts, setting a goal in

---

1. Ashish K. Jha et al., *How Common Are Electronic Health Records in the United States? A Summary of the Evidence*, HEALTH AFF. w496, w504 (2006), http://content.healthaffairs.org/cgi/content/full/25/6/w496 ("[T]he best evidence, based on independent, high-quality surveys, suggests that as of 2005, approximately 24 percent of physicians used an EHR [Electronic Health Record]."); Julie Bell, *Old School, New Vision; Making Way for the Future: A Hopkins Surgeon Yields to Change, Prepares Proteges as He Caps His Career*, BALT. SUN, Aug. 14, 2006, at 1A.
2. *See* Jha et al., *supra* note 1.
3. TASK FORCE TO STUDY ELEC. HEALTH RECORDS, MD. HEALTH CARE COMM'N, HEALTH INFORMATION EXCHANGE 10 (2006) [hereinafter HEALTH INFORMATION EXCHANGE].
4. *See* COMM. ON QUALITY OF HEALTH CARE IN AMERICA, INST. OF MED., TO ERR IS HUMAN: BUILDING A SAFER HEALTH SYSTEM 1 (Linda T. Kohn et. al. eds., National Academy Press 2000) [hereinafter TO ERR IS HUMAN].
5. *See* Jha et al., *supra* note 1, at w503; *see also infra* Part III.A.5.
6. RelayHealth, https://www.relayhealth.com/rh/specific/patients/onlineServices/whatCanDo.aspx (last visited Sept. 15, 2008). The patient-centric changes mimic the conveniences financial institutions increasingly have allowed, giving customers the option of paying bills or checking bank balances via the Web. Press Release, Pew Internet & American Life Project, Online Banking Jumps 47% in Two Years (Feb. 2005) [hereinafter Pew Internet & American Life Project], *available at* http://www.pewinternet.org/pdfs/PIP_Online_Banking_2005.pdf.

2004 of making patients' health records electronic by 2014.[7] President Barack Obama has said he is committed to the same goal.[8]

Despite this years-long national push, the effort to create an electronic medical record that health-care providers may share across health systems is moving slowly.[9] Health-care providers such as hospitals disagree on how to implement it and struggle to pay for record systems that can "talk" to each other.[10] Patients apparently do not want to wait.[11] In a development that has ramifications for efficiency, public health, and medical privacy, patients are beginning to share medical information via the Web, alone or with the help of products Microsoft and others have launched.[12] These new models of sharing health information are primed to grow in popularity because they are driven by the free market, do not rely on grant funding, and do not require health-care institutions to agree on how to implement them.[13]

These new models include Web sites which host companies operate much like a blend between the Facebook social networking site and the PayPal electronic payment service.[14] As with Facebook, individuals who sign up choose what content to store on the site.[15] But on Facebook, the information individuals load—whether images or written information—is automatically placed onto a publicly

---

7. Julie Hirschfeld Davis, *Bush to Visit Baltimore Veterans Center; President to Promote Plan to Computerize U.S. Medical Records*, BALT. SUN, Apr. 27, 2004, at 3A.
8. Robert Pear, *Privacy Issue Complicates Push to Link Medical Data*, N.Y. TIMES, Jan. 18, 2009, at A16 (quoting President Obama as saying, "We will make the immediate investments necessary to ensure that within five years all of America's medical records are computerized.").
9. Julia Adler-Milstein et al., *The State of Regional Health Information Organizations: Current Activities and Financing*, HEALTH AFFAIRS w60, w66–w69 (2007), *available at* http://www.mendocinohre.org/rhic/200712/hlthaff27-1-w60v1.pdf.
10. TASK FORCE TO STUDY ELEC. HEALTH RECORDS, MD. HEALTH CARE COMM'N, FINAL REPORT 21–25 (2007) [hereinafter TASK FORCE FINAL REPORT].
11. *See* LAKE RESEARCH PARTNERS, AM. VIEWPOINT & MARKLE FOUND., SURVEY FINDS AMERICANS WANT ELECTRONIC PERSONAL HEALTH INFORMATION TO IMPROVE OWN HEALTH CARE (2006), http://www.markle.org/downloadable_assets/research_doc_120706.pdf.
12. *Id.*; *see also* Steve Lohr, *Microsoft Offers System to Track Health Records*, N.Y. TIMES, Oct. 5, 2007, at C3; TASK FORCE FINAL REPORT, *supra* note 10, 3–4, 8.
13. *See infra* Part V.A.3.
14. *See* Facebook Principles, http://www.facebook.com/policy.php?ref=pf (last visited Dec. 1, 2008); Privacy Policy for PayPal Services (Including PayPal Money Market Fund), http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy-outside (last visited Dec. 1, 2008).
15. *See* Facebook Principles, *supra* note 14.

visible Web page to which individuals may restrict access by adjusting privacy settings.[16] The new PayPal-like health-information sites have no automatically public face.[17]

Web sites such as Microsoft's HealthVault, launched in 2007,[18] are an example. Via HealthVault, individuals upload, store, and share their health information.[19] The idea is that another person can see an individual's health information on HealthVault only if the individual grants that person permission.[20] When individuals assemble and upload medical information for their own benefit, the result is a personal health record, or PHR.[21] The new sites have the potential to do what years of government and private-industry efforts have been unable to accomplish—the digital compiling of an individual's health history in a single spot, ready for instantaneous sharing.[22] But as individuals gain control of their health information in one way, by obtaining it from health-care providers who traditionally have held it, they may be losing control of it in another way, by making their information susceptible to public exposure.[23] If the new model gains in popularity as some health information technology watchers

16. *See id.*
17. Telephone Interview with George Scriban, Product Manager, HealthVault (March 7, 2008); E-mail from George Scriban, Product Manager, HealthVault, to Matthew Jacobson, University of Baltimore Law Review Editor in Chief (Sept. 24, 2008) (on file with author); Privacy Policy for PayPal Services, *supra* note 14.
18. Press Release, Microsoft Corp., Microsoft Unveils Consumer Health Vision, Launches Technology Platform to Collect, Store and Share Health Information (Oct. 4, 2007), *available at* http://www.microsoft.com/presspass/press/2007/oct07/10-04HealthVaultPR.mspx.
19. *Id.*; *see also* Telephone Interview with George Scriban, *supra* note 17.
20. Telephone Interview with George Scriban, *supra* note 17.
21. *See infra* Part III.D.2. There is no single, agreed-upon definition of "personal health record" (PHR), and various employers, caregivers, insurers, and others offer platforms for them. Janlori Goldman, *Personal Health Records: Employers Proceed with Caution*, ISSUE BRIEF (Cal. HealthCare Found., Oakland, Cal.) Jan. 2007, at 1–2 ("[Personal Health Records] should be distinguished from electronic health record systems (EHRs). While both offer the functionality to collect health information about an individual, PHRs focus on providing information of value to consumers, while EHRs focus on informing clinical practice and facilitating claims handling.").
22. *See* TASK FORCE FINAL REPORT, *supra* note 10, at 2–3; *see also* Ann Bagchi et al., *Considerations in Designing Personal Health Records for Underserved Populations*, ISSUE BRIEF (Mathematical Policy Research, Inc., Princeton, N.J.), Apr. 2007, at 1.
23. Bob Brown, *The Number of Online Personal Health Records Is Growing, but Is the Data in These Records Adequately Protected?*, J. HEALTH CARE COMPLIANCE 35, 36 (2007).

predict,[24] patients' health records increasingly will move on electronic highways that are outside of recently implemented medical confidentiality regulations.[25]

The Health Insurance Portability and Accountability Act of 1996 (HIPPA) mandated federal regulations to protect the confidentiality of individuals' health information.[26] Resulting regulations, generally encompassed in HIPAA's Privacy and Security rules, began taking effect in 2001 and had rolling compliance deadlines that stretched into 2008.[27] But the regulations apply only to individually identifiable health information stored or transmitted by "covered entities," which generally consist of health insurers, health-care clearinghouses that process billing information, and health-care providers.[28] The rules therefore are widely interpreted not to encompass Web site providers managing individuals' health information at the individuals' request.[29] Whether the personal health information stored on these new Web sites also is outside the reach of the Maryland Confidentiality of Medical Records Act is an untested question.[30]

The answer is important in part because medical information is both highly personal and big business.[31] Medical information companies already use de-identified pharmacy data, for example, to

24. Jane Sarasohn-Kahn, *Get Out the Crystal Ball: Predicting What's Next for Health IT*, iHEALTHBEAT, Dec. 20, 2007, *available at* http://www.ihealthbeat.org/articles/2007/12/20/Get-Out-the-Crystal-Ball-Predicting-Whats-Next-for-Health-IT.aspx?topicID=54.

25. *See* Brown, *supra* note 23, at 35–36.

26. Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. FED. 133, 133 (2004).

27. *Id.* at 145–150; Compliance Dates of the Implementation of the Standard Unique Health Identifier for Health Care Providers, 45 C.F.R. § 162.404 (2005). Some scholars define confidentiality and privacy differently, with confidentiality generally referring to the expectation that those to whom data is entrusted in confidence will not redisclose it. *See infra* notes 285–89 and accompanying text. Privacy, for purposes of this Comment, means "providing individuals some level of information and control regarding the uses and disclosures of their personal information." Peter P. Swire & Lauren B. Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515, 1518 (2002).

28. *See* Brown, *supra* note 23, at 35–36; *see also* 45 C.F.R. §§ 160.102, 164.104 (2005).

29. *See* Brown, *supra* note 23, at 35–36.

30. *See* MD. CODE ANN., HEALTH-GEN. § 4-301 (LexisNexis 2007). The act has been operative since 1991 and is applicable to those who redisclose medical information as well as those who husband it. § 4-302.

31. Mike Hatch, *HIPAA: Commercial Interests Win Round Two*, 86 MINN. L. REV. 1481, 1490–91 (2002).

track drug prescriptions, providing pharmaceutical companies, Wall Street analysts, and others with information about demand without disclosing consumers' identities.[32] Drug companies covet information about the frequency of particular diseases and the basis for consumer preferences for particular treatments.[33]

PHR sites conceivably provide a way for companies to reach consumers with advertising, including advertisements seeking to entice them to enroll in clinical trials testing experimental drugs the companies are developing for consumers' ailments.[34] In this way, the sites could play a role in ensuring that drug companies develop useful drugs.[35] PHR sites also open up an avenue for potential privacy abuses.[36] The disclosure of medical information, whether inadvertent or not, can lead to embarrassment, ostracism, job loss, difficulty obtaining health insurance, and health-care fraud.[37]

This Comment analyzes the privacy of personal health records, with a focus on Maryland law. Part II of this Comment details the historical, constitutional, common law, and statutory bases for medical privacy in Maryland. Part III explores the forces leading to the development of personal health records and how they are distinct from traditional electronic medical records. Part IV analyzes personal health records under existing law and concludes such records do not enjoy protection under HIPAA or the Maryland Confidentiality of Medical Records Act. Part V examines the contracts under which vendors promise to protect the personal health information that consumers store on their sites. Part VI explores the dangers of medical privacy breaches for patients and recommends

32. One prominent example is IMS Health, the New York Stock Exchange-traded company which describes itself as "the world's leading provider of market intelligence to the pharmaceutical and healthcare industries." Press Release, IMS Health, IMS Health Reports U.S. Prescription Sales Grew 3.8 Percent in 2007, to $286.5 Billion (Mar. 12, 2008) [hereinafter IMS Health], *available at* http://imshealth.com/portal/site/imshealth (follow "Press Room" hyperlink; then click on "News Releases" hyperlink; go to "2008" on the drop down menu, and then scroll down).

33. *See* IMS Health *supra* note 32 and accompanying text.

34. *See infra* Part V.A.3.a–b.

35. *See infra* Part V.A.3.b.

36. *See infra* Parts V and VI.

37. *See* Hatch, *supra* note 31, at 1490 ("There has never been a more important time to safeguard our medical privacy. The rapid growth of marketing databases, the regular news of accidental or purposeful disclosure of sensitive health information, and the potential misuse of such information to deny credit, employment, or insurance coverage has never been greater.").

that the Maryland General Assembly take action to assure personal health record privacy.

II. THE DEVELOPMENT OF MEDICAL PRIVACY LAW IN MARYLAND

A. The Historical Bases of Medical Privacy

"Privacy—and the right of the individual to embrace dignity—is considered an essential ingredient to individual autonomy and a free society."[38] "Stripped of privacy, the citizen is subjected to embarrassment by neighbors, discrimination by employers, and humiliation from friends and relatives."[39] Medical records often contain "intimate and personal" information,[40] making access to them and protection of them particularly important to autonomy.[41]

The earliest privacy protections for medical information were based not on the law, but on professional ethics.[42] "Since the time of Hippocrates, doctors have sworn to maintain the confidentiality of sensitive information, in order to establish a trusting relationship with their patients."[43] Such ethical practices were designed at a time when medical practice generally entailed interactions between a patient and a single doctor.[44]

---

38. *Id.* at 1486.
39. *Id.*
40. *Id.* at 1489.
41. *See* Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y L. & ETHICS 327, 328 (2002).
42. *Id.*
43. *Id.*
44. *Id.*

> Ethical justifications for privacy frequently begin with the ancient Hippocratic Oath that admonishes physicians to disclose personal information. . . . However, most health data are not directly disclosed by patients or held by treating physicians. Rather, data are generated from multiple sources such as laboratories, pharmacies, and research. Data are also used by many entities such as employers, insurers, and managed care organizations. In a complex modern world, data cannot be maintained tightly within the bounds of a single patient/physician relationship.

Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1448 (2002).

B. The Constitutional Right to Medical Privacy in Maryland

Maryland's highest court has recognized a broad right to the privacy of medical records under the U.S. Constitution.[45] It did so despite the fact that "[t]he United States Supreme Court has not directly held" that there is such a right.[46] The Supreme Court has, however, "assumed that the right of privacy founded on the Fourteenth Amendment concept of personal liberty . . . encompasses an interest in avoiding disclosure of personal matters . . . ."[47] In certain instances, the Supreme Court has found a right to medical privacy.[48] For example, when the U.S. Court of Appeals for the Fourth Circuit found that testing pregnant women for cocaine did not constitute an unreasonable search under the Fourth Amendment, the Court overruled the decision, finding that "[i]n that context, . . . individuals have a 'reasonable expectation of privacy' in their medical information."[49]

Maryland courts have held that the constitutional right to medical privacy is not absolute.[50] In *Dr. K. v. State Bd. of Physician Quality Assurance*, the Court of Special Appeals of Maryland adopted a test crafted by the Third Circuit to determine whether a state actor, in this case the board charged with policing physicians, manifests a compelling state interest that outweighs an individual's constitutional right to medical privacy.[51] The Court of Appeals of Maryland has

---

45. Doe v. Md. Bd. of Soc. Work Exam'rs, 384 Md. 161, 183–86, 862 A.2d 996, 1008–10 (2004) (detailing the U.S. Supreme Court's presumption in Whalen v. Roe, 429 U.S. 589, 599–600 (1977), that individuals have a constitutional privacy right in avoiding the disclosure of personal matters and holding that "[m]edical records fall within the protections of this right to privacy."); *see also*, Md. State Bd. of Phys. v. Eist, 176 Md. App. 82, 932 A.2d 783 (Ct. Spec. App. 2007) (detailing constitutional and statutory bases for the medical right to privacy in Maryland); Dr. K. v. State Bd. of Phys. Quality Assurance, 98 Md. App. 103, 111–12, 632 A.2d 453, 457 (Ct. Spec. App. 1993).

46. *Eist*, 176 Md. App. at 97 n.8, 932 A.2d at 792 n.8.

47. *Id.* (citing *Whalen*, 429 U.S. at 600).

48. *Id.* (citing Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001)).

49. *Id.* The precise language of the Supreme Court opinion, which the Court of Special Appeals of Maryland here interprets, says "The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent." *Ferguson*, 532 U.S. at 78.

50. *Eist*, 176 Md. App. at 116–17, 932 A.2d at 803–04 (adopting the multifactor balancing test the Third Circuit used in U.S. v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980)).

51. 98 Md. App. 103, 112, 632 A.2d 453, 458 (Ct. Spec. App. 1993) (applying the multifactor test in *Westinghouse*, 638 F.2d at 577–78).

adopted the test.[52] The test weighs the government's competing interest by considering:

> [T]he type of record requested, the information it contains, the potential for harm in subsequent nonconsensual disclosure, the injury in disclosure to the relationship for which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the government's need for access, and whether there is an express statutory mandate, articulate public policy, or other public interest militating towards access.[53]

C. *Common Law Protections for Medical Records in Maryland*

Maryland courts have strengthened the protections inherent in a physician's ethical duty of confidentiality by recognizing a common law duty.[54] Consequently, "absent a statute permitting otherwise, the patient has a right to assume that his medical condition will not voluntarily be disclosed by the provider to other persons without the patient's consent."[55]

As with the constitutional protections for individuals' medical privacy, the common law confidentiality protection is not absolute.[56] "In general, if a patient is on notice that a medical encounter will

---

52. Doe v. Md. Bd. of Soc. Work Exam'rs, 384 Md. 161, 186, 862 A.2d 996, 1010 (2004).

53. *Id.* at 185, 862 A.2d at 1009 (quoting *Dr. K*, 98 Md. App. at 114–15, 632 A.2d at 459). In *Doe v. Maryland Board of Social Work Examiners*, the Court of Appeals of Maryland denied a motion by a clinical social worker's clients to quash a subpoena for their treatment records after the social worker was accused of failing to report that one of them was suspected of sexually abusing a child. *Id.* at 166–67, 862 A.2d at 998–99. While the case involved mental health records and a social worker, not physical health records and a physician, the court ruled broadly, finding the multifactors test "applied in *Dr. K*, is the correct standard to use when balancing individual privacy interests in medical records against competing state interests in those records." *Id.* at 186, 862 A.2d at 1010. It found that the state's compelling interest in protecting the public by investigating a licensed social worker's failure to report suspected child abuse outweighed the clients' privacy interests. *Id.* at 188–89, 862 A.2d at 1011–12.

54. Lemon v. Stewart, 111 Md. App. 511, 525, 682 A.2d 1177, 1183 (Ct. Spec. App. 1996) ("[T]he relationship between a health care provider and its patient is one of trust and confidence.").

55. *Id.*

56. *See* Medical Records—Application of Maryland Medical Records Confidentiality Act to a Possible Statewide "Health Information Exchange" Mechanism, 92 Md. Op. Att'y Gen. 107, 112 (2007).

entail third-party disclosure and continues with the provider, consent is implied and so the disclosure does not breach the physician's duty."[57]

Like many states,[58] Maryland also recognizes the tort of invasion of privacy based on unreasonable public disclosure of private facts.[59] But, as Joy L. Pritts noted in a 2002 analysis, the success rate of plaintiffs who bring such tort claims "has been extremely low" given that they must prove the disclosure "would be highly offensive to a reasonable person."[60]

D. Statutory Protections for Medical Privacy in Maryland

1. Federal Law

At least twelve major federal laws protect personal health information in various situations.[61] Four apply to government agencies handling medical information, while seven others protect health information in limited situations.[62] Perhaps the most widely applicable protections are encompassed in HIPAA's Privacy Rule.[63]

> [T]he Privacy Rule creates national standards to keep individuals' medical records and other personal health information confidential. It restricts and defines the ability of health plans, health care clearinghouses, and most health care providers [collectively known as "covered entities" under the law] to divulge patient medical records. Furthermore, it generally guarantees patient access to medical records and imposes a deadline of 30 days by which

57. *Id.*
58. Pritts, *supra* note 41, at 331.
59. Pemberton v. Bethlehem Steel Corp., 66 Md. App. 133, 166, 502 A.2d 1101, 1118 (Ct. Spec. App. 1986).
60. Pritts, *supra* note 41, at 331.
61. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO–07–238, HEALTH INFORMATION TECHNOLOGY: EARLY EFFORTS INITIATED BUT COMPREHENSIVE PRIVACY APPROACH NEEDED FOR NATIONAL STRATEGY app. V (2007) [hereinafter GAO REPORT].
62. *Id.* For example, the Social Security Act requires the U.S. Health and Human Services Department, the Social Security Agency and its contractors to protect individually identifiable health information, while the Financial Modernization Act of 1999 prohibits financial institutions, including certain health insurers, from disclosing consumers' nonpublic personal information to unaffiliated third parties without the consumers' consent. *Id.*
63. 45 C.F.R. § 164.500. HIPAA is applicable to data regardless of whether it is held by the government or private sector. *See* 45 C.F.R. § 160.102; *see also* Buckman, *supra* note 26, at 133.

> access must be provided, unless the information is not maintained or accessible on site.[64]

The privacy regulations require covered entities sharing personal health information with each other to "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits."[65] The regulations also cover "business associate[s]," those with whom covered entities contract regarding handling of personal health information.[66] The government can fine violators, but the law does not allow individuals to sue privately for damages.[67]

HIPAA's privacy provisions remain so new that there is little case law interpreting them. It was not until 2003 that covered entities had to comply with HIPAA's Privacy Rule.[68] To date, HIPAA regulations have withstood constitutional challenges.[69]

2. State Law

The major state statute safeguarding individual medical records is the Maryland Confidentiality of Medical Records Act, which preceded HIPAA by taking effect in 1991.[70] The act mandates that "[a] health care provider shall: (1) Keep the medical record of a patient or recipient confidential; and (2) Disclose the record only: (i) As provided by this subtitle; or (ii) As otherwise provided by law."[71] It also mandates that "[a] person to whom a medical record is disclosed may not redisclose the medical record to any other person unless the redisclosure is" otherwise permitted by the law or permitted by certain listed exceptions.[72] If convicted, a health-care provider who "knowingly and willfully violates" the act "is guilty of a misdemeanor" and "subject to a fine" of up to $1,000 "for the first offense" and up to $5,000 "for each subsequent conviction."[73]

---

64. Buckman, *supra* note 26, at 149 (citing 45 C.F.R. § 164.524(b)(2)).
65. 45 C.F.R. § 164.306(a)(1).
66. § 160.103.
67. Buckman, *supra* note 26, at 149, 171 (citing O'Donnell v. Blue Cross Blue Shield of Wyo., 173 F.Supp. 2d 1176 (D. Wyo. 2001)).
68. *Id.* at 148.
69. *Id.* at 163, 165–66 (citing Ass'n of Am. Phys. & Surgeons, Inc. v. U.S. Dep't of Health & Human Servs., 224 F.Supp. 2d 1115 (S.D. Tex. 2002); S.C. Medical Ass'n v. Thompson, 327 F.3d 346 (4th Cir. 2003)).
70. MD. CODE ANN., HEALTH-GEN. §§ 4-301–09 (LexisNexis 2005).
71. § 4-302(a).
72. § 4-302(d).
73. § 4-309(d).

3. HIPAA Generally Does Not Preempt the State Act

Congress dictated when it passed HIPAA in 1996 that the regulations the U.S. Health and Human Services Department ultimately wrote to implement HIPAA "would 'not supersede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than'" the federal regulations.[74] The Maryland Attorney General's Office has advised that HIPAA supplements, but generally does not supersede, Maryland's statute.[75]

4. Sharing of Medical Records Among Providers Without Explicit Patient Consent

While no court has ruled on the issue, the Maryland Attorney General's Office issued an opinion in August 2007 advising that the state's Confidentiality of Medical Records Act allows health-care entities covered by the law to agree to share patient information *with each other in the future* without patients' explicit consent.[76] The opinion also concluded that patients who consent to be seen by one participating provider could not "opt out" of such future information-sharing even if they objected.[77] The opinion came as regional health-care providers discussed whether to develop a health information exchange.[78] An exchange is one way providers such as hospitals and physicians' offices can share electronic records documenting each encounter with a particular patient.[79] The exchange presumably would entail software that would allow providers to quickly check a database listing all providers who have seen the patient they are now treating and—depending on the model ultimately decided upon—either download detailed records of those encounters from a central database or request them from the earlier provider(s) to see what was done.[80]

---

74. Buckman, *supra* note 26, at 149 (quoting HIPAA, Pub. L. No. 104–191, § 264 (codified at 42 U.S.C.A. § 130d-2 (West 2003))).
75. 92 Md. Op. Att'y Gen. 107, 110 (2007); *see also* 88 Md. Op. Att'y Gen. 205 (2003) ("In practice, the HIPAA regulations do not effect a wholesale federal preemption of the field of medical record privacy, but rather establish a national floor of medical privacy protection.").
76. 92 Md. Op. Att'y Gen. 107, 114.
77. *Id.* at 114–15.
78. *Id.* at 107.
79. *Id.*; *see also* TASK FORCE FINAL REPORT, *supra* note 10, at 90.
80. 92 Md. Op. Att'y Gen. 107; *see also* TASK FORCE FINAL REPORT, *supra* note 10, at 90.

The Attorney General's Office concluded providers may share patient information through such a system based on a statutory provision that allows providers to share information with their agents and employees, "so long as the sole purpose of the disclosure is the 'offering, providing, evaluating, or seeking payment for health care to patients . . . by the provider.'"[81] The Attorney General's opinion suggested that HIPAA would not bar such unauthorized sharing because the federal regulation has "analogous" provisions.[82]

The opinion did not address a number of questions regarding certain kinds of electronic health information. Even presuming that a Maryland court would agree that information accessible among providers falls within current federal and Maryland privacy protections, would that protection extend to instances where patients obtain their own health information from a provider, then upload it onto a privately run portal such as HealthVault? What if a health-care provider electronically sends a patient's medical records, at the patient's request, directly to a personal health records Web site with which the provider has no "business associate" agreement under HIPAA? What if the patient supplements a providers' medical record with his or her own thoughts and observations, making the medical information a hybrid of that provided by the health-care institutions and that provided by the patient? No court has addressed such instances, though they presumably are occurring as free-market sites try to satisfy patients' desire to have the same electronic access to, and electronic control of, their health information as they do over money in their bank accounts.[83]

III. FORCES LEADING TO DEVELOPMENT OF PERSONAL HEALTH RECORDS; HOW THEY DIFFER FROM THE MEDICAL RECORDS PROVIDERS KEEP

To understand why it is important to update relatively recent laws protecting electronic health information, it is first important to understand two things: (1) the market for personal health records is developing as the trend toward sharing traditional electronic medical records across health systems falters,[84] and (2) there are differences between health records now being assembled on personal health sites

81. 92 Md. Op. Att'y Gen. 107, 114 (citing MD. CODE ANN., HEALTH-GEN. § 4-305(b)(1) (LexisNexis 2005)).

82. *Id.* at 114 n.11 (citing 45 C.F.R. §§ 164.502(a)(1)(ii), 164.506 (2007)).

83. Telephone Interview with George Scriban, *supra* note 17.

84. *See infra* Part III.C.

such as HealthVault and the medical records health-care providers keep.[85]

A. Forces Driving the Trend Toward Electronic Medical Records

1. The Cost of Health Care

"Health-care spending accounted for 16[%] of gross domestic product in 2006,"[86] and health-care spending grew at an annual rate of 6.7%—more than twice the nation's 3.2% general inflation rate.[87] The result: those who pay for health care, including the government through its $401.3 billion a year federal Medicare program for the elderly[88] and its $310.6 billion a year Medicaid program for the indigent,[89] and private employers who sponsor employee health-insurance programs, are looking for ways to cut health-care costs.[90] Some studies have suggested that shifting from paper records to electronic medical records may be an effective way of decreasing costly medical mistakes.[91] As a result of the belief that health information technology, which relies on the conversion from paper to electronic medical records, will help health-care payers save money by increasing efficiency, the growing market for health-care information-related products is projected to be at least $34.7 billion by 2011.[92]

---

85. *See infra* Part III.D.

86. Christopher Lee, *Medicare Helps Push Drug Spending Up*, WASH. POST, Jan. 8, 2008, at A3.

87. Press Release, Centers for Medicare & Medicaid Services, CMS Reports U.S. Health Care Spending Growth Accelerated Only Slightly in 2006, but Still Faster Than Economic Growth and General Inflation (Jan. 8, 2008), *available at* http://www.cms.hhs.gov/apps/media/press/release.asp?counter=2810.

88. Lee, *supra* note 86.

89. *Id.*

90. President Bush, for example, cited the goal of reducing health-care costs, among other things, in ordering the creation of "an interoperable health information technology infrastructure" that would make use of electronic patient information. Exec. Order 13,335, 3 C.F.R. 160–61 (2005), *reprinted in* 42 U.S.C. § 300u (Supp. IV 2007). On the private-sector side, The Leapfrog Group represents large employers aiming to improve the "quality and affordability of health care" partly by encouraging physicians to write prescriptions electronically. The Leapfrog Group, Fact Sheet, http://www.leapfroggroup.org/media/file/The_Leapfrog_Group_Fact_Sheet_03_2008.pdf (last visited Sept. 26, 2008).

91. *See, e.g.*, FIRST CONSULTING GROUP, COMPUTERIZED PHYSICIAN ORDER ENTRY: COSTS, BENEFITS AND CHALLENGES 3 (2003), *available at* http://www.leapfroggroup.org/media/file/Leapfrog-AHA_FAH_CPOE_Report.pdf.

92. Jane M. Von Bergen, *Poised to Assist the Medical Sector in . . . Connecting the Data*, PHILA. INQUIRER, Jan. 21, 2007, at E1 ("BBC Research & Consulting, a Denver

2. The Advent of Personalized, Genetic Medicine

The sequencing of the human genome has led to the advent of personalized medicine, in which physicians are accelerating an effort to tailor treatment based on individuals' genetic variations.[93] As genetic analysis plays an increasingly important role in diagnosis and treatment, the amount of information incorporated into the practice of medicine is exploding.[94]

Genentech's Herceptin became one of the first therapies targeted at a specific genetic variation.[95] It won government marketing approval in 1998 for treatment of a breast cancer characterized by too much of a protein involved in regulating cell growth.[96] Now companies are considering marketing genetic-information tools directly to consumers.[97] Recently, for example, a company called 23andMe, "announced plans to provide affordable chunks of their DNA to individual consumers, along with tools to help them keep track of and understand their genetic information."[98]

3. A Shift in the Practice of Medicine from Solo to Teamwork

The increasing complexity of medicine has led to a shift from the days in which a single physician interacted with a single patient to one in which teams of specialists cooperate to diagnose and treat patients.[99] The change is exemplified by Johns Hopkins' treatment of pancreatic cancer, in which Johns Hopkins surgeon John Cameron specializes.[100] Where treatment once involved decisions made by a dominant surgeon given almost god-like reverence, advances in the understanding of the underlying disease mean a team comprised of an oncologist, radiation oncologist, pathologist, surgeon, and others now

---

market-research firm, predicts that the market for health-information technology will reach $34.7 billion in sales by 2011—and that does not include computer systems used by insurers, employers or even individuals to keep track of their care.").

93. *See, e.g.*, Andrew Pollack, *Genetic Test to Give Clues on Treatment of Hepatitis C*, N.Y. TIMES, Apr. 26, 2006, at C3.

94. *See, e.g.*, Andrew Pollack, *A Crystal Ball Submerged in a Test Tube: Genetic Technology Reshapes the Diagnostics Business*, N.Y. TIMES, Apr. 13, 2006, at C1.

95. *See, e.g.*, Genentech, Herceptin, http://www.gene.com/gene/products/information/oncology/herceptin (last visited Sept. 26, 2008).

96. *See, e.g.*, Imaginis, Breast Cancer Treatment: HER2, Herceptin, and TyKerb, http://www.imaginis.com/breasthealth/herceptin.asp (last visited Sept. 26, 2008).

97. Amy Harmon, *6 Billion Bits of Data About Me, Me, Me!*, N.Y. TIMES, June 3, 2007, § 4, at 1.

98. *Id.*

99. Bell, *supra* note 1.

100. *Id.*

cooperate to evaluate the best course of treatment for each patient.[101] With similar changes happening across medicine,[102] it is increasingly important that physicians and other caregivers cooperating in a patient's treatment be able to quickly share and review medical information pertinent to that particular patient.

4. The Mobility of Patients

About 14% of Americans, or 40 million people, move annually,[103] often presumably necessitating a change in health-care providers. Americans also switch jobs often: the average person born during the latter part of the baby boom held 10.8 jobs from ages 18 to 40.[104] Such switches may necessitate a change in health plans, which often differ from company to company. Some Americans also travel out of the country for medical care.[105] Mobility arguably contributes to the need for medical records that are easily accessible from wherever a patient may be or that can easily travel with him or her.

5. A Desire to Reduce Medical Errors

Concern over harmful medical errors is also driving a push for increased use of what the health-care industry calls health information technology.[106] Several Institute of Medicine studies, including one that estimated between 44,000 and 98,000 Americans die each year as a result of medical errors in hospitals,[107] have prompted the health-care industry and those who pay for care to focus on ways of reducing such errors.[108] Many of the solutions

101. *See id.*
102. *See id.*
103. Press Release, U.S. Census Bureau, Moving Rates Lowest in 50+ Years (Mar. 23, 2004) (citing U.S. CENSUS BUREAU, GEOGRAPHICAL MOBILITY: 2002 TO 2003 (2004)), *available at* http://www.census.gov/Press-Release/www/releases/archives/mobility_of_the_population/001729.html.
104. U.S. DEP'T OF LABOR, BUREAU OF LABOR STATISTICS, NUMBER OF JOBS HELD, LABOR MARKET ACTIVITY, AND EARNINGS GROWTH AMONG THE YOUNGEST BABY BOOMERS: RESULTS FROM A LONGITUDINAL SURVEY (June 27, 2008), *available at* http://www.bls.gov/news.release/pdf/nlsoy.pdf.
105. *All Things Considered: Employers, Insurers Consider Overseas* (National Public Radio broadcast Nov. 14, 2007), *available at* http://www.npr.org/templates/story/story.php?storyId=16294182.
106. TASK FORCE FINAL REPORT, *supra* note 10, at 8.
107. *Id.* at 7 (citing TO ERR IS HUMAN, *supra* note 4, at 1, 26, 31).
108. *Id.* at 17–19; *see also* The Leapfrog Group, Fact Sheet, http://www.leapfroggroup.org/about_us/leapfrog-factsheet.pdf (last visited Sept. 22,

involve better use of computers in health care for reasons as simple—and as important—as the fact that many errors result when those administering medicine misread the handwriting of those prescribing it.[109]

As a result, groups such as The Leapfrog Group, a consortium of employers who pay much of the health-insurance costs for their employees,[110] have called for wider use of software programs that allow physicians to enter prescriptions into a handheld device at the bedside.[111] Such devices can allow doctors to see a patient's abbreviated medical record in electronic form and emit automatic warnings on the screen if a doctor enters a prescription that may negatively interact with a medicine the patient already is on or enters a dose that is too high.[112]

6. Patients' Familiarity with Electronic Banking and Shopping

Consumers increasingly are using Web sites to research and conduct many of the transactions in their everyday lives, laying the foundation for their ability to use electronic health-care information—whether they are patients or physicians.[113] Some 53 million people used some form of online banking in November 2004, up 47% from the 37 million who did so in 2002, according to a survey by the Pew Internet & American Life Project.[114] Such sites generally allow customers to check their bank balances and post and pay bills.[115]

Customers also can buy and sell stocks through online brokerages; compare mortgage rates or insurance rates; research and compare home prices in a particular area, as well as compare the cost of living across state lines; research the gas mileage, maintenance rates, resale values and prices of particular makes and models of cars; listen to,

---

2008) ("A 1999 report by the Institute of Medicine gave the Leapfrog founders an initial focus—reducing preventable medical mistakes.").

109. *See* Robert Pear, *Clinton to Order Steps to Reduce Medical Mistakes*, N.Y. TIMES, Feb. 22, 2000, at A1; *see also* David C. Classen et al., *Evaluation and Certification of Computerized Provider Order Entry Systems*, 14 J. AM. MED. INFORMATICS ASS'N, 48, 51 (2007), *available at* http://www.pubmedcentral.nih.gov/articlerender.fcgi?tool=pubmed&pubmedid=17077453.

110. The Leapfrog Group, Fact Sheet, http://www.leapfroggroup.org/media/file/leapfrog_factsheet.pdf (last visited Sept. 22, 2008).

111. *Id.* (referring to such devices as Computer Physician Order Entry (CPOE)).

112. *See* Classen et al., *supra* note 109, at 48–49 (describing the alert function as "decision support").

113. *See* Pew Internet & American Life Project, *supra* note 6, at 1–2.

114. *See id.* at 1.

115. *See* Bank of America, https://www.bankofamerica.com (last visited Sept. 22, 2008).

buy, and download music; shop online via the Web sites of many brick-and-mortar retailers; shop for virtually anything via the eBay online flea market; and find out what their friends are doing or viewing on social networking sites such as MySpace, where hosts can control who sees what.[116]

B. Government and Private Industry Respond as Health Care Industry's Use of Information Technology Lags Other Industries

While the health-care industry makes use of sophisticated technology to diagnose and treat patients, it has moved slowly compared to industries such as banking when it comes to turning records from paper into electronic form.[117] Through 2005, only about 24% of physicians working in walk-in clinics (as opposed to hospitals) used electronic medical records, while just 5% of hospitals used electronic prescribing.[118]

1. The Federal Government Responds

Concerned about rising costs, high medical error rates, and the inability of consumers to comparison shop for health care, the government in recent years has taken a number of actions to encourage the health-care industry to adopt more widespread use and sharing of electronic medical records.[119] In April 2004, for example, President Bush issued an executive order establishing a national health information technology coordinator.[120] The order assigned the coordinator to come up with a strategic plan to develop a "nationwide interoperable health information technology infrastructure" that, among other things, "[r]educes health care costs resulting from

116. *See, e.g.*, E*Trade Financial, http://www.us.etrade.com/e/t/home (last visited Sept. 22, 2008); Bankrate.com, http://www.bankrate.com (last visited Sept. 22, 2008); Insurance.com, http://www.insurance.com (last visited Sept. 22, 2008); Cyberhomes, http://www.cyberhomes.com (last visited Sept. 22, 2008); Economic Research Institute, http://www.eriei.com (last visited Sept. 22, 2008); Kelly Blue Book, http://www.kbb.com (last visited Sept. 22, 2008); Emusic, http://www.emusic.com (last visited Sept. 22, 2008); Macy's, http://www.macys.com (last visited Sept. 22, 2008); eBay, http://www.ebay.com (last visited Sept. 22, 2008); MySpace, http://www.myspace.com (last visited Sept. 22, 2008).

117. *Compare* Jha et al., *supra* note 1, at w504 (five percent of hospitals used electronic prescribing through 2005) *with* Pew Internet & American Life Project, *supra* note 6, at 1 ("Fifty-three million people, or 44% of Internet users and one-quarter of all adults" reported using online banking as of late November 2004).

118. Jha et al., *supra* note 1.

119. Exec. Order No.13,335, 3 C.F.R. 160, 160–61 (2005).

120. *Id.* at 160.

inefficiency, medical errors, inappropriate care, and incomplete information . . . [and] [p]romotes a more effective marketplace, greater competition, and increased choice through a wider availability of accurate information on health care costs, quality and outcomes."[121] The President said the initiative's goal was to have the system of shareable electronic records operable nationwide by 2014.[122] The American Health Information Community, a federal advisory panel chartered in 2005 to advise the government on how to achieve the goal, selected "consumer empowerment" and a standardized electronic health record as two of four initial areas upon which to concentrate.[123] The advisory panel said its initial consumer empowerment goal is to ensure consumers have access to "a consumer-directed and secure electronic record of health care registration information and a medication history."[124] Its broader goal, however, is to ensure "wide spread adoption of a personal health record."[125]

2. Maryland State Government Responds

In May 2005, the Maryland General Assembly sought guidance by establishing the Maryland Task Force to Study Electronic Health Records and ordering it to report on the current use and potential expansion of such records in Maryland.[126] In 2007, the General

121. *Id.* at 161.

122. U.S. Dep't of Health & Human Servs., Office of the National Coordinator: Background, http://www.hhs.gov/healthit/onc/background (last visited Sept. 22, 2008) ("[It's] the President's goal for most Americans to have access to an interoperable electronic medical record by 2014.").

123. U.S. Dep't of Health & Human Servs., American Health Information Community: Breakthroughs, http://www.hhs.gov/healthit/community/breakthroughs (last visited Sept. 22, 2008) (listing the other two goals as improving "chronic care" and "biosurveillance," for example, by transferring de-identified data from health-care providers to public health officials within 24 hours). Plans are under way for a public-private partnership to continue the work of the federal advisory committee. U.S. Dep't of Health & Human Servs., Health Information Technology: The AHIC Successor is Launched, http://www.hhs.gov/healthit/community/background/AHICsuccessor.html (last visited Dec. 1, 2008).

124. *Id.*

125. U.S. Dep't of Health & Human Servs., Consumer Empowerment Workgroup, http://www.hhs.gov/healthit/ahic/consumer (last visited Sept. 8, 2008) (reporting the American Health Information Community's recommendation that personal health records should be "easy-to-use, portable, longitudinal, affordable, and consumer-centered.").

126. 2005 Md. Laws 1506–08.

Assembly established a pilot project under which regional health-care providers would share electronic information with each other.[127]

3. Private Industry Responds in Cooperation with Government

Across the United States, thirty-two regional medical records sharing Health Information Exchanges (HIE) were "fully operational in 2007," according to the eHealth Initiative Foundation's Fourth Annual Survey of State, Regional, and Community-Based Health Information Exchange Initiatives.[128] Generally, health information exchanges allow providers to share information about each patient by, for example, storing certain patient information in a central database that all providers can log into and view.[129] The HIE task force describes the enormous potential benefits of such medical-records sharing:

> In the ideal vision of HIE's future, consumers who switch physicians or insurers, or who seek emergency care, will no longer suffer from delayed or lost medical records. The benefits of HIE would be far reaching: efficient and dependable HIE would reduce redundant laboratory tests for patients who seek care in different settings, reduce duplication of radiology studies through digital transmission of reports, enable reliable connections to pharmacies to help generate better medication lists, and reduce adverse effects from drug interactions. HIE could also be used to improve the referral process and communication between providers, and transitional care (such as between clinic and hospital) would be safer for all patients.[130]

C. *Information-Sharing Initiatives Falter Given Major Hurdles*

1. Health Information Exchanges Struggle Financially; Many Fail

While there is wide agreement that sharing information would cut health-care costs by increasing efficiency and improve patient care,[131] there are signs that the health information exchanges, and the

127. 2007 Md. Laws 1748.
128. eHealth Initiative, 2007 HIE Survey: Key Findings, http://www.ehealthinitiative.org/2007HIESurvey/ (last visited Sept. 22, 2008).
129. *See* HEALTH INFORMATION EXCHANGE, *supra* note 3, at 1.
130. *Id.* at 1–2.
131. *Id.*

organizations set up to establish them, are faltering.[132] A 2007 survey of 145 regional organizations trying to set up data exchanges showed "nearly one in four of them were defunct [and] only twenty were functioning at even a modest scale."[133] Most early successes involved the exchange of test results.[134] The survey authors conclude their findings raise concerns about the ability of the current approach to achieve widespread clinical data exchange.[135]

2. Maryland Organization Is Among Those That Gave Up

The Maryland/D.C. Collaborative for Health Information Technology, a non-profit established in May 2004, is among those that voted to disband its fledgling regional health information organization.[136] The collaborative hoped the organization would link "all components of the Maryland/D.C. health care delivery area—physician offices, hospitals, clinics, labs, imaging centers, nursing homes, payers and patients—for secure and appropriate exchange of health information."[137] The group also hoped to determine whether exchanging data was economically sustainable, would improve the quality and safety of patient care, and would decrease costs.[138] Although the group involved thirty-five major health-care organizations, including Johns Hopkins Medicine, the University of Maryland Medical System, CareFirst BlueCross BlueShield, and Aetna, as well as community physicians and hospitals,[139] it was never able to attract sufficient funding to extensively plan or implement a system.[140] Its members voted to disband the regional health information organization in June 2007.[141]

3. A Litany of Typical Problems

The Maryland/D.C. Collaborative's problems appear to be typical. The Task Force detailed a number of barriers to successful electronic information-sharing within and among providers, including financial

132. Adler-Milstein et al., *supra* note 9, at w66.
133. *Id.*
134. *Id.* at w68.
135. *See id.* at w68–w69.
136. TASK FORCE FINAL REPORT, *supra* note 10, at 15.
137. *Id.*
138. HEALTH INFORMATION EXCHANGE, *supra* note 3, at 12.
139. TASK FORCE FINAL REPORT, *supra* note 10, at 15.
140. HEALTH INFORMATION EXCHANGE, *supra* note 3, at 12.
141. TASK FORCE FINAL REPORT, *supra* note 10, at 15.

barriers, legal concerns, physician resistance, technology barriers, and consumer trust and confidence.[142]

a. Financial barriers

The Task Force reported on December 31, 2007, that the high cost of implementing electronic health records leads some providers to avoid making the switch from paper to software.[143] The preliminary planning for a health information exchange that shares records across providers costs $300,000 to $1,000,000,[144] while the development and implementation phases can run anywhere from $3,000,000 to $10,000,000.[145] Providers are expected to pay these costs and buy the technology to make exchanging health information possible, while insurers, employers, and government purchasers of health care reap the benefits of lower costs.[146] The potential for increased legal costs, as the next section discusses, is a related concern.

b. Legal concerns and physician resistance

Health-care institutions and private physicians are concerned that electronic records in general and information-sharing in particular will increase the costs associated with complying with privacy regulations, increase the chances that private health-information inadvertently will be disclosed, and potentially create exposure to new liabilities associated with health information technology.[147] For example, doctors are concerned that if they exercise their judgment to prescribe a medication after an electronic prescribing program warns against it for reasons the doctors think inapplicable, they may open themselves up to medical malpractice claims.[148] Doctors also worry that their work will be interrupted by having to make computer entries, that they will be interacting with computers and not people, and that they may not be paid for this computer time.[149]

142. *Id.* at 21–26.
143. *Id.* at 21–22.
144. HEALTH INFORMATION EXCHANGE, *supra* note 3, at 5.
145. *Id.*
146. TASK FORCE FINAL REPORT, *supra* note 10, at 38 ("The health care reimbursement system today is designed to pay providers for procedures and episodic clinical care, but not to reimburse for health care coordination or information management, which leads to quality improvement.").
147. *Id.* at 23.
148. *Id.*
149. *See id.* at 24–25.

Another legal problem that plagued the development of earlier data-sharing initiatives may stymie health information exchanges, as well: it is not clear who owns the data once it is shared.[150] The legal uncertainty about ownership may make some medical institutions more likely to jealously guard information because of a perceived proprietary stake.[151]

c. Technology barriers

Different providers have different electronic records systems that cannot "talk" to each other,[152] that do not have all the capabilities required to exchange and analyze information, and that are constantly changing with continuously evolving software because the field is so new.[153]

d. Consumer trust and confidence

"[C]onsumers are key to the acceptance of" health information technology.[154] But currently, consumers are worried that electronic sharing of their information will result in "inappropriate access to medical information, which could result in the loss of employment or insurance."[155] At least one study has shown consumers' lack of trust is particularly high among racial minorities, who prefer paper records.[156]

"Trust, privacy, security, and consumer control of their information are key issues that need to be addressed if [health information technology] is to gain broad consumer acceptance."[157] In fact, the task force concluded that consumer interest in an alternative form of information sharing has been increasing, driven by the fact that many of the current models that providers and the government are exploring have "limitations in making data available to the consumer."[158] One alternative form is the personal health record.

150. HEALTH INFORMATION EXCHANGE, *supra* note 3, at 9 ("Health institutions highly value information, because it is information that drives their business.").
151. *Id.*
152. TASK FORCE FINAL REPORT, *supra* note 10, at 23.
153. *Id.* at 24.
154. *Id.* at 25.
155. *Id.*
156. *See* Bagchi et al., *supra* note 22, at 2–3.
157. TASK FORCE FINAL REPORT, *supra* note 10, at 25.
158. *Id.* at 30.

D. There Are Generally Recognized Differences Between Electronic Medical Records and Personal Health Records

The definitional differences between personal health records and electronic medical records, discussed in this section *infra*, are important for determining whether statutes designed to protect the confidentiality of medical records also protect personal health records.

1. Various Industry Definitions of an Electronic Medical Record

Many industry definitions of the term "electronic medical record" either state or presume that its custodian is a health-care provider or associated entity.[159] The American Health Information Management Association defines an electronic medical record as, "the computerization of health record content and associated processes usually referring to an electronic medical health record in a physician office setting or a computerized system of files."[160] The Maryland Task Force to Study Electronic Health Records, the entity the Maryland General Assembly formed in 2005 to study the "current and potential expansion of electronic health record utilization in the State,"[161] settled upon an expanded definition for the purposes of its report and called the expanded medical records form an "electronic health record," or EHR.[162] According to the task force, an electronic health record has "five leading characteristics."[163] It (1) longitudinally collects electronic health information for and about individuals; (2) is kept in a unified system along with the health information of multiple individuals; (3) offers authorized users immediate electronic access to individual's information; (4) serves as each individual's legal medical record; and (5) is maintained by individual medical providers (e.g., physicians and other caregivers, hospitals, nursing homes, and clinics).[164]

159. *Id.* at 28.
160. *Id.*
161. Letter from Peter Basch, Chair of the Task Force to Study Elec. Health Records, to Md. Governor Martin O'Malley and Members of the Md. Gen. Assembly (Dec. 19, 2007), *reprinted in* TASK FORCE FINAL REPORT, *supra* note 10.
162. TASK FORCE FINAL REPORT, *supra* note 10, at 29.
163. *Id.*
164. *Id.*

2. Various Definitions of a Personal Health Record (PHR)

Most industry definitions of a personal health record either state or presume that it is controlled by the patient (sometimes referred to as the health-care "consumer"), or state that it should be controlled by the patient.[165] The American Health Industry Management Association defines a personal health record as "an electronic, universally available, lifelong resource of health information needed by individuals to make health decisions."[166] The task force put forth the proposition that personal health records "aggregate [personal] health information into one location that is controlled by the consumer."[167]

In a January 2007 Issue Brief published by the California HealthCare Foundation, Health Privacy Project Director Janlori Goldman defined personal health records in part by distinguishing them from electronic health records: "PHRs focus on providing information of value to consumers, while EHRs focus on informing clinical practice and facilitating claims handling."[168]

A PHR can exist in many different forms, both electronic and paper. It can be as simple as a form created by an individual to record important medical information or as complex as a Web-based system accessed and populated by patients, health-care providers, insurers, pharmacies, employers, and companies providing health-related content. Information in a PHR may include family history, medication and immunization registers, lab results, digital images of tests (such as mammograms and MRIs), claims data, health assessments, drug interaction warnings, drug refill reminders, guidance aimed at managing or preventing a particular condition or disease, and resources for locating and rating physicians and hospitals. A PHR can be created and maintained by individual patients, their caregivers, or family members.[169]

---

165. *See, e.g.*, Goldman, *supra* note 21, at 1; TASK FORCE FINAL REPORT, *supra* note 10, at 30; AHIMA e-Him Personal Health Record Work Group, *The Role of the Personal Health Record in the EHR*, J. AHIMA, July-Aug. 2005, at 64A–D [hereinafter AHIMA], *available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_027539.hcsp?dDocName=bok1_027539.

166. AHIMA, *supra* note 165.

167. TASK FORCE FINAL REPORT, *supra* note 10, at 30 (citing Brett Brune, *Medical Data: A Personal Health Record Is an Effort to Pull All of Your Information into One Usable Source*, HOUSTON CHRON., Sept. 6, 2006, at D1).

168. Goldman, *supra* note 21.

169. *Id.* at 1.

3. Different Kinds of Entities Are Starting Personal Health Record Systems to Store Individuals' Records for Them to Use

Among companies that have created personal health record systems or plan to do so are WebMD, the health-information Web site; Google, the company best known for its search engine; and Revolution Health Group, which operates a WebMD competitor.[170] Also in the market are Microsoft's HealthVault,[171] McKesson Corporation's RelayHealth,[172] and insurers Aetna[173] and Kaiser Permanente.[174] The companies are examples of the variety of different kinds of entities that are starting personal health record systems. In time, more private employers may offer or encourage the use of personal health record sites.[175] As Goldman states:

> A PHR system can be offered and managed by employers for the benefit of their workforce, providing for a [large] range of access and control by employees, as well as providers, payers, and content providers. A PHR can be portable, stored on a card or a USB drive and viewed or edited by plugging the device into a computer at home or at the point of care, or it can be Web-based and accessible via the Internet.[176]

4. Maryland Task Force Suggests Wait and See Approach

With all of these efforts in their infancy, the Maryland Task Force to Study Electronic Health Records has taken the position that the state should not respond to the movement until it is clear how the market for personal health records will develop.[177] To support its position, the task force cites a Health Industry Insights Consumer Survey published in May 2006 that found "83% of 1,095 consumers

170. *See* HEALTH PRIVACY PROJECT, OVERVIEW: BEST PRACTICES FOR EMPLOYERS OFFERING PERSONAL HEALTH RECORDS (PHRS) 2 (2007), *available at* http://www.healthprivacy.org/files/Best_Practices_Overview.pdf.

171. HealthVault, www.healthvault.com (last visited Oct. 2, 2008).

172. RelayHealth, http://www.relayhealth.com (last visited Oct. 2, 2008).

173. Press Release, Aetna, Aetna Introduces Powerful, Interactive Personal Health Record (Oct. 3, 2006), *available at* http://www.aetna.com/news/2006/pr_20061003.htm.

174. Press Release, Kaiser Permanente, Kaiser Permanente Puts Personal Health Record Front and Center (Nov. 6, 2007), *available at* http://ckp.kp.org/newsroom/national/archive/nat_071106_myhealthmanager.html.

175. *See* TASK FORCE FINAL REPORT, *supra* note 10, at 72.

176. Goldman, *supra* note 21, at 1.

177. TASK FORCE FINAL REPORT, *supra* note 10, at 4.

surveyed had no experience with PHRs. Approximately 90% of those who created a PHR did so using paper or common computer applications, such as a word processing application; they did not use a specific PHR software product."[178] Simultaneously, however, the task force notes that what is holding the market back is the very regulatory, legislative, and legal uncertainty it declines to address: "In order for PHRs to be accepted and used," the task force's report notes, "there must be clearly defined data ownership rights, privacy obligations, and identification of potential liabilities for all stakeholders."[179]

Dr. Peter Basch, who has used electronic medical records in his internal medicine practice for more than a decade, is nonetheless wary of accessing electronic personal health records.[180] Basch, who chaired the Maryland Task Force to Study Electronic Health Records, but emphasized he was speaking for himself, said one unresolved issue is whether a physician who acquires access to a personal health record from a patient may simultaneously be creating a legal duty to know what is in it.[181] Because patients may frequently update personal health records, there is the danger that even the most diligent doctor may fail to see an entry.[182] Patients also have the ability to alter test results in their personal health records.[183] They may fear their insurer or employer could find out a "bad" result if it is included in such a record. Thus the records arguably are less reliable than electronic medical records doctors keep.[184] Lastly, electronic personal health records may be disorganized or unnecessarily lengthy, causing time-pressed doctors to waste minutes or even hours wading through irrelevant information.[185]

"If we could get beyond that," Basch said of the concerns, "most doctors could learn to accept with a grain of salt what they get" in a personal health record.[186]

While the number of people using electronic personal health records is small,[187] it is clear that influential public and private forces

178. *Id.* at 30.
179. *Id.*
180. Telephone Interview with Peter Basch, Internal Medicine Doctor (Mar. 4, 2008). Basch practices in Washington, DC.
181. *Id.*
182. *Id.*
183. *Id.*
184. *Id.*
185. *Id.*
186. *Id.*
187. TASK FORCE FINAL REPORT, *supra* note 10, at 30–31.

support their development.[188] In addition to the American Health Information Community federal advisory panel, which supports consumer control of personal health information,[189] companies such as Google and Microsoft also are investing in the trend.[190]

Joanne Pollak, general counsel for Johns Hopkins Medicine, is among those pondering the legal ramifications of the trend.[191] She compared the health-care industry's current reticence to that of music labels which initially resisted but ultimately facilitated consumers' desire to download music to create their own collections.[192] "We all have to figure it out," Pollak said of finding a safe way for consumers and practitioners to use personal health records: "It's going to happen."[193]

IV. CURRENT PRIVACY LAW DOES NOT APPEAR TO COVER PERSONAL HEALTH RECORDS

A. Personal Health Record Systems Are Not "Covered Entities"

HIPAA applies only to covered entities, defined as health-care providers, health-care clearinghouses, insurers and their business associates.[194] There is widespread agreement that it does not cover entities that operate personal health records systems when they have contracted directly with consumers and are not handling the information via a business associate agreement with a covered entity.[195] A number of organizations and individuals already have noted the hole in the regulations.[196]

B. Personal Health Records Under Maryland Law

The issue of whether the privacy of personal health records is protected under Maryland law has never been adjudicated. The

188. *See supra* note 170 and accompanying text.
189. *See supra* note 125 and accompanying text.
190. Mary Vanac, *Clinic Is Pilot for Google Medical Data Interface*, PLAIN DEALER (Cleveland), Feb. 22, 2008, at C1.
191. Interview with Joanne Pollak, Gen. Counsel, Johns Hopkins Med. (Dec. 31, 2007).
192. *Id.*
193. *Id.*
194. *See* 45 C.F.R. §§ 160.102–03 (2005).
195. *See* Brown, *supra* note 23, at 36; *see also* Goldman, *supra* note 21, at 3; William S. Bernstein et al., *Whose Data Is It Anyway?*, ISSUE BRIEF (Cal. HealthCare Found., Oakland, Cal.) Feb. 2008, at 4–5.
196. *See* Brown, *supra* note 23, at 36; *see also* Goldman, *supra* note 21, at 3; Bernstein et al., *supra* note 195.

following provides a novel analysis of the status of personal health records under Maryland law.

1. Traditional Physician Ethical Protections Do Not Apply

When patients decide to store their personal health records outside the control of their health-care providers, such as on HealthVault's Web site, they almost certainly are placing them in an arena where the physician's ethical duty to protect the records does not apply.[197] In fact, the proliferation, computerization, and electronic transfer of medical records increasingly is leading to situations in which "[m]any . . . holders of health information are not subject to ethical obligations to maintain its confidentiality."[198]

2. At Most, Personal Health Records Have Limited Constitutional Protection

Even if a court were to find personal health records should be treated analogously to legal medical records under Maryland statutes (a question analyzed *infra*), personal health information would be highly unlikely to enjoy more privacy protection under the U.S. Constitution than do the medical records which health-care providers hold.

Maryland's highest court has held that medical records "fall within the protections" of the federal constitutional right to privacy, but that they must nonetheless be disclosed to a state actor, such as a panel that oversees social workers, given a compelling state interest.[199] The ruling of the Court of Appeals of Maryland in *Doe v. Maryland Board of Social Work Examiners* concerned records of individual counseling sessions between a clinical social worker and her clients.[200] But the Court ruled broadly as it adopted the Third Circuit's *Westinghouse* balancing test for determining when a state actor has a compelling interest that outweighs the individual right to privacy in medical records.[201] The court stated:

> We agree with the intermediate appellate court that the balancing test framework described in *Westinghouse* . . . is the correct standard to use when balancing individual

197. *See* Pritts, *supra* note 41, at 328–29.
198. *Id.* at 328.
199. Doe v. Md. Bd. of Soc. Work Exam'rs, 384 Md. 161, 183, 185–86, 862 A.2d 996, 1008–10 (2004).
200. *Id.* at 166–67, 862 A.2d at 998–99.
201. *Id.* at 186, 862 A.2d at 1010.

> privacy interests in medical records against competing state interests in those records. Whether a compelling state interest can be shown in order to override an individual's privacy interest is to be determined on a case-by-case basis.[202]

The ruling appears to encompass all medical records a state actor seeks, not just mental health records held by a psychiatrist or social worker.[203] It is difficult to foresee a circumstance in which personal health records that a patient creates and voluntarily agrees to house on a Web site, ostensibly to facilitate the sharing of the records with selected others, would be accorded more constitutional protection than medical records a provider houses.[204]

3. Traditional Common Law Medical Privacy Protections Inapposite

Common law confidentiality laws barring physician disclosure of medical information do not appear to cover situations in which a consumer obtains his or her own information from a doctor and then transfers it to a Web site.[205] Under Maryland common law, a patient's consent is a defense to a medical privacy violation.[206] In *Lemon v. Stewart*, the Court of Appeals of Maryland held that, "absent a statute permitting otherwise, the patient has the right to assume that his medical condition will not voluntarily be disclosed by the provider to other persons without the patient's consent."[207] The *Lemon* court did not distinguish among means of disclosure, so consent would appear to immunize a provider who electronically transfers a patient's medical record directly to a personal health record site at the patient's request.[208] Even in situations in which a physician does not have specific consent to transfer a particular patient record, the Maryland Attorney General's Office has noted: "In

---

202. *Id.* (citations omitted).
203. *See id.*
204. *See id.*
205. *See infra* notes 206–09 and accompanying text.
206. *See* Lemon v. Stewart, 111 Md. App. 511, 525, 682 A.2d 1177, 1183 (Ct. Spec. App. 1996). There is some question whether a health-care provider's electronic transfer of a medical record to a personal health records site would constitute disclosure under the law, given that providers likely could argue they are simply giving the information to the patient and no one else. *See id.* at 525 (listing the statutory requirement to notify *the patient* of positive HIV test results).
207. *Id.*
208. *See id.*

general, if a patient is on notice that a medical encounter will entail third-party disclosure and continues with the provider, consent is implied and so the disclosure does not breach the physician's duty."[209] Whether consent to transfer a record to a patient's personal health records portal would constitute disclosure would depend on the facts of a particular case.

4. Maryland Confidentiality of Records Act Does Not Apply

Unlike the HIPAA regulations,[210] the Maryland Confidentiality of Medical Records Act does not mention electronic medical records anywhere in its text, necessitating statutory analysis to determine whether it nonetheless encompasses both traditional electronic medical records and personal health records.[211]

a. The statute's plain language does not resolve whether electronic personal health records are considered medical records for purposes of the statute and therefore covered by it

i. The statute covers medical records in electronic form

The "starting point in every case involving construction of a statute is the language itself."[212] The statute defines "medical record" as:

> [A]ny oral, written, or other transmission in any form or medium of information that: (i) Is entered in the record of a patient or recipient; (ii) Identifies or can readily be associated with the identity of a patient or recipient; and (iii) Relates to the health care of the patient or recipient.[213]

The statute defines "health care" as: "[A]ny care, treatment, or procedure by a health care provider: (1) To diagnose, evaluate, rehabilitate, manage, treat, or maintain the physical or mental condition of a patient or recipient; or (2) That affects the structure or function of the human body."[214] It defines "health care provider" in part as: "A person who is licensed, certified, or otherwise authorized under the Health Occupations Article or . . . § 10-101(e) of this

209. 92 Md. Op. Att'y Gen. 107, 112 (2007).
210. 45 C.F.R. § 164.306(a)(1) (2007).
211. *See* MD. CODE ANN., HEALTH-GEN. §§ 4-301 to -309 (LexisNexis 2005).
212. Kaczorowski v. Mayor of Balt., 309 Md. 505, 514, 525 A.2d 628, 632 (1987) (quoting Watt v. Alaska, 451 U.S. 259, 265–66 (1981)).
213. MD. CODE ANN., HEALTH-GEN. § 4-301(h)(1)(i)–(iii) (LexisNexis 2005).
214. § 4-301(f)(1)–(2).

article, a hospital . . . a related institution . . . a health maintenance organization . . . an outpatient clinic . . . and a medical laboratory."[215]

It mandates that the term "includes the agent, employees, officers, and directors of a facility and the agents and employees of a health care provider."[216]

While the definition of medical record does not specifically cite electronic forms, the plain language of the statute appears to encompass electronically transmitted information within its broad definition: "[A]ny oral, written, or other transmission in any form or medium of information . . . ."[217] The Maryland Attorney General's Office, in an advisory opinion, has so found, advising:

> [A]lthough medical records in electronic form may have been uncommon when the Act became law, the definition's comprehensive phrasing ("any form or medium of information") means that the Act encompasses paper records themselves, the electronic embodiment of paper records after scanning or some other imaging process, and records initially created in electronic form.[218]

ii. The statute's plain language does not appear to cover PHRs

The term "personal health record" is not mentioned in the statute.[219] The statute requires a "health care provider" to: "(1) Keep the medical record of a patient or recipient confidential; and (2) Disclose the medical record only: (i) As provided by this subtitle; or (ii) As otherwise provided by law."[220] It also provides: "A person to whom a medical record is disclosed may not redisclose the medical record to any other person unless the redisclosure is: (1) Authorized by the person in interest; (2) Otherwise permitted by this subtitle" or permitted under two other exceptions.[221] The law's plain language

215. § 4-301(g)(1)(i)–(ii).
216. § 4-301(g)(2).
217. § 4-301(h)(1).
218. 92 Op. Md. Att'y Gen. 107, 111 (2007).
219. § 4-301.
220. § 4-302(a)(1)–(2).
221. § 4-302(d)(1)–(4) (Supp. 2007). The other two exceptions are those permitted under § 1-202(b) or (c) of the Human Services Article, which concern reports of child abuse and neglect, and directory information, defined in § 4-301(b)(1) as "information concerning the presence and general health condition of a patient who has been admitted to a health care facility or who is currently receiving emergency health care in a health care facility."

does not resolve whether the General Assembly meant to cover redisclosure of medical information that a health-care provider created when documenting treatment of a patient, where the provider subsequently released the information to an entity with which the patient contracts to house it along with other information.[222]

One key, then, to determining whether Maryland's privacy protections extend to electronic personal health information redisclosed by a custodian such as a website is whether a personal health record constitutes a "medical record" for purposes of the statute in the first place. If a personal health record is not encompassed within the definition of "medical record," a Web site that "rediscloses" it is not in violation of Maryland's statute. On the other hand, if a personal health record is considered a medical record, other considerations come into play.[223] One is what statutorily covered privacy rights patients give up, if any, by posting health information to the Web site. Encompassed in this question is the issue of who owns the personal health information: the health-care provider who created it, the patient to whom it pertains, or the Web site that ultimately posts it under an agreement with the patient.[224]

The term "personal health record" is not mentioned in the statute.[225] The law's plain language does not resolve whether the General Assembly meant to cover redisclosure of medical information that a health-care provider created when documenting treatment of a patient, where the provider subsequently released the information to an entity with which the patient contracts to house it along with other information.[226] Arguably, a personal health record is synonymous with a "medical record" if a patient's personal health record involves medical information a provider entered into the patient's medical record that identifies her and relates to any "care, treatment, or procedure by a health care provider"[227]—regardless of where that information is now stored and whether other information is stored with it. The question remains: Does the medical record lose its statutorily protected status—and therefore its protection upon redisclosure—depending on where it is housed and what is housed with it?

222. § 4-301(e).
223. *See supra* notes 206–09 and accompanying text.
224. *See* TASK FORCE FINAL REPORT, *supra* note 10, at 30.
225. § 4-301.
226. § 4-301(e).
227. § 4-301(f)–(h).

iii. Canons of statutory construction allow 'external' evidence

Maryland canons of statutory construction allow a court to look outside the precise language of the code to determine a statute's meaning.[228] If the legislature intended the statute to encompass medical information found in what is now known as a "personal health record," a court might find that the statute covers "personal health records."[229] The key to understanding a statute's purpose is seeing the "light of the statute's context."[230] In determining the purpose, a court is not limited to the statute's words, but "must consider other 'external manifestations' or 'persuasive evidence,' including a bill's title and function paragraphs, amendments that occurred as it passed through the legislature, its relationship to earlier and subsequent legislation, and other material that fairly bears on the fundamental issue of legislative purpose or goal . . . ."[231]

The purpose statement and preamble of the Maryland Confidentiality of Medical Records Act, which contain similar language, also are not dispositive, though they appear to be referring in context to records a health-care provider holds.[232] The purpose statement says the act is:

> For the purpose of providing for the confidentiality of medical records; authorizing disclosure of certain medical records under certain circumstances; requiring a health care provider to establish certain procedures for the addition to or correction of a medical record; authorizing a health care provider to require certain persons to make certain payments; repealing a certain provision on disclosure of medical records of individuals in certain facilities; defining certain terms; providing certain exceptions; providing certain immunity under certain circumstances; providing for certain liability under certain circumstances; establishing certain penalties; providing for a delayed effective date; and generally relating to the confidentiality of medical records.[233]

228. Kaczorowski v. Mayor of Balt., 309 Md. 505, 514–15, 525 A.2d 628, 632–33 (1987).
229. *See id.* at 516, 525 A.2d at 633.
230. *Id.*
231. *Id.* at 515, 525 A.2d at 632.
232. Maryland Confidentiality of Medical Records Act, 1990 Md. Laws 2023–24.
233. *Id.* at 2023.

The legislative history of Senate Bill 584 shows the General Assembly considered the Maryland Confidentiality of Medical Records Act amid concern that personal medical records were increasingly likely to be compromised as more entities handled the information using "automated information systems."[234] The Senate Economic and Environmental Affairs Committee initially began study of the issue during the 1989 session, concerned solely with a departmental bill that sought to establish a new system governing disclosure of mental health records.[235] "The bill resulted from confusion surrounding who could have access to mental health records and under what circumstances,"[236] according to a Floor Report. The report provided this background:

Because of the serious emotional, physical, and financial harm to an individual that may result from the improper disclosure of all types of health-care information, the Health Subcommittee expanded its study of Senate Bill 133 to include the revision of current law that governs the confidentiality of personal medical records. The increasing use of party payment plans, the expanding use of health-care information for education, research and quality assurance purposes, the increasing involvement of government agencies in many aspects to health care, and the expanding use of automated systems have created numerous opportunities for confidential information to be compromised. However, the confidentiality of medical records must be balanced against the legitimate need of certain entities, such as government agencies and third party payors, to access this information.[237]

Senator Paula C. Hollinger, the bill's sponsor, said in her written testimony that:

> This bill is setting new ground rules for all health care providers in this state. . . . [it] strikes a balance between the desire of consumers of health care to have strong penalties in the bill in order to have available remedies when the confidentiality of a medical record is compromised versus

234. S. COMM. ON ECON. AND ENVTL. AFFAIRS, FLOOR REPORT, S.B. 584, at 3 (Md. Gen. Assem. 1990) [hereinafter FLOOR REPORT].

235. *Id.*

236. *Id.*

237. *Id.*

> the providers who do not wish to be heavily penalized for an inadvertent mistake.[238]

A Summary Sheet for Senate Bill 584 notes that the bill is significant because it provides disclosure provisions for providers as well as facilities. "Only facilities are covered in current law," the undated summary notes.[239]

The General Assembly debated the bill at a time when concern remained high about the spread of HIV.[240] AIDS activists were among those testifying in favor of it, noting the discrimination those with the disease—and mistakenly identified as having the disease—were encountering at work and elsewhere.[241] Amid the backlash against those suffering from AIDS, U.S. Health and Human Services Secretary Otis R. Bowen encouraged states to consider medical records confidentiality legislation covering "all persons and medical records, not just those that are AIDS-related."[242]

A 1987 press release in which Bowen encouraged states to take that action,[243] along with a letter he wrote to governors[244] making the same suggestion, were among the materials submitted to the Committee considering Maryland Senate Bill 584.

The legislative history behind the Maryland Confidentiality of Medical Records Act indicates that legislators foresaw the increasing automation of medical records and risk of confidential information being exposed.[245] They also noticed that others, such as insurers and hospitals, increasingly were using medical records for things unrelated to direct care of patients, such as billing, and wanted to ensure confidentiality by those "agents" of health-care providers, as well.[246] Lastly, the history indicates legislators were concerned about

---

238. *Maryland Confidentiality of Medical Records Act: Hearing on S.B. 584 Before the S. Comm. of Econ. and Envtl. Affairs* (Md. 1990) [hereinafter *Hearing*] (statement of Sen. Paula C. Hollinger).

239. Summary Sheet, S.B. 584.

240. *See supra* notes 218–21 and accompanying text.

241. *Hearing*, *supra* note 238 (statement of Stuart Harvey, AIDS Partnership Council Legislative Committee representative).

242. Press Release, U.S. Dep't of Health & Human Servs., HHS Sec'y Otis R. Bowen, M.D., Today Asked Governors Throughout the Nation to Share Information (Oct. 26, 1987) (on file with author).

243. *Id.*

244. Form letter from Otis R. Bowen, Sec'y of the U.S. Dept. of Health & Human Servs., to "Dear Governor [blank]" (Oct. 21, 1987) (on file with author).

245. *See* FLOOR REPORT, *supra* note 234.

246. Maryland Trial Lawyer's Assoc., S.B. 584, Medical Records Committee Recommended Changes or Additions (Md. 1990).

redisclosure of medical information by the individuals who handled it, given the emerging discrimination against people with AIDS.[247]

Despite their foresight, however, there is no indication that legislators anticipated situations in which patients themselves would amalgamate medical records from different health-care providers and create a record distinct from anything held by any one individual provider. The language and history of Senate Bill 584 instead shows it was aimed at medical records created and held by providers or their agents, not at information released to patients who then put it to use themselves.[248] It is therefore unlikely a court would find that the Maryland Confidentiality of Medical Records Act extends to personal health records when patients have gathered the information themselves, or requested that providers forward it electronically to patients' personal health records sites.[249]

V. IN MANY CASES, PERSONAL HEALTH RECORDS APPEAR PROTECTED ONLY BY PRIVACY STATEMENTS

The primary protection for the privacy of personal health records that patients store on Web sites appears to be each vendor's privacy statement.[250]

A. The Example of Microsoft's HealthVault

HealthVault's site, for example, displays this notice: "You control your health information. You decide who can share it, and what they can share. We always ask for consent before allowing another person or Web site to access health information."[251]

1. HealthVault's Privacy Statement

HealthVault's privacy statement implicitly acknowledges that the site collects some data from users, noting the statement "applies to the data collected by Microsoft through the Microsoft HealthVault beta version."[252] It is difficult to tell from HealthVault's privacy

247. *See supra* notes 219–22 and accompanying text.

248. *See* FLOOR REPORT, *supra* note 234.

249. *See* Kaczorowski v. Mayor of Balt., 309 Md. 505, 516, 525 A.2d 628, 633 (1987) (finding legislative purpose, "determined in light of the statute's context," is the key to ascertaining a statute's meaning).

250. *See infra* Part V.A–B.

251. HealthVault, Welcome to Microsoft HealthVault, http://healthvault.com/Personal/index.html (last visited Oct. 5, 2008).

252. HealthVault, Microsoft HealthVault Account Beta Version Privacy Statement, https://account.healthvault.com/help.aspx?topicid=PrivacyPolicy&rmproc=true (last visited Dec. 2, 2008).

statement alone what data Microsoft and various affiliated "Programs" collect.[253] Under the heading "Collection of your personal information," the privacy statement notes that a HealthVault customer may use the same e-mail address and password to sign into other Microsoft accounts, as well as those of "select" Microsoft partners, and refers customers to the Microsoft Online Privacy Statement to learn how Web sites use their credential information.[254] The Microsoft Online Privacy Statement contains references to other "Supplemental Privacy Information" that may apply.[255] The HealthVault privacy statement notes that a customer can use "Programs" to enter health information and "give 'Programs' permission to view, add, modify and/or delete information in a [HealthVault] record."[256] For information on how each "program" uses a customer's e-mail address, as well as what other customer information a program may collect and how the program may use that information, HealthVault's privacy statement directs the customer to view "each program's" privacy statement.[257] The result is that customers must view multiple privacy statements to understand how all of the entities involved will store, access, transfer, collect, or use customers' information.[258]

2. What HealthVault Collects from Users

HealthVault Product Manager George Scriban said Microsoft does not currently collect health data from its users and will not do so

253. *See id.*

254. *Id.* (stating that, "[w]hen you sign in using Live Windows ID, we refer to the e-mail address and password you use as your Windows Live ID or your Microsoft Passport Network credentials").

255. Microsoft Online Privacy Statement, http://privacy.microsoft.com/en-us/fullnotice.mspx (last visited Dec. 1, 2008).

256. HealthVault, *supra* note 252.

257. *Id.* (noting that "[t]he Service provides links to each Program's privacy statements at the time the Service asks you to authorize the Program's access").

258. *Id.* Microsoft also repeatedly updates the privacy statement, meaning the privacy statement changes. The version of the Microsoft HealthVault Account Beta Version Privacy Statement in use as of December 2008 listed various differences from those in effect in October 2007, June 2008, and September 2008. *Id.* The most recent version makes it clear—for those willing to read well into a privacy statement that runs more than seven printed pages—how easily customers can lose control of their own health record if they are not careful. *Id.* For example, the statement notes that, if a HealthVault customer grants "custodian" access to another person, such as a spouse or other relative, that "custodian can also revoke access to a record from any other custodian of the record, *including you*." *Id.* (emphasis added).

without clearly asking permission for a specific purpose.[259] He said in a March 2008 interview that the data that the company acknowledges collecting in its privacy statement refers only to the data Microsoft needs to properly administer the HealthVault service, such as page views at particular times of day.[260] The data helps Microsoft determine such things as when to perform maintenance on the site.[261] He said the site-administration data the company collects "is not associated with any personally identifiable information."[262] HealthVault's privacy statement makes clear that Microsoft may aggregate individuals' data and use it to market HealthVault to potential advertisers.[263] The HealthVault privacy statement promises that the data advertisers see will not reveal anything specific about any particular individual's account.[264]

3. HealthVault's Strategy for Making Money

a. The current strategy solely focuses on advertising

HealthVault does not charge users.[265] It brings in revenue by selling advertising that consumers see when they use Live Search Health—a Google-like search function for health information that users can access on the HealthVault.com home page.[266] HealthVault's current strategy is to become the primary platform for personal health records, leading customers to use Microsoft's search engine to find health-care information on the Web.[267] While far less popular than Google, the search engine could become vastly more popular and attract more advertisers if the strategy works.[268] Individuals do not need a HealthVault account to use Live Search Health.[269]

259. Telephone Interview with George Scriban, *supra* note 17.
260. *Id.*
261. *Id.*
262. *Id.*
263. HealthVault, *supra* note 252.
264. *Id.*
265. Telephone Interview with George Scriban, *supra* note 17.
266. *Id.*
267. *Id.*
268. *Id.*
269. Microsoft HealthVault Beta, http://www.healthvault.com/Personal/index.html (for Live Search Health Results, click in search box labeled "Web health results" in upper right hand corner, type in term to be searched and hit "enter" on your keyboard) (last visited Mar. 7, 2009).

HealthVault also allows companies such as LifeScan, Inc. to interface with the consumers free of charge.[270] LifeScan makes a blood-sugar monitor used for managing diabetes.[271] Like a number of other devices, LifeScan's monitor is compatible with HealthVault software.[272] This allows consumers to load the results of each blood test into their HealthVault personal health record[273] and make it available to anyone they choose. HealthVault has myriad other partners as well. For example, it has launched pilot programs with hospitals, including one in which patients sign a permission form that allows the hospital to electronically send their discharge summary directly to their HealthVault personal health record.[274]

b. HealthVault's attitude toward "data-mining" in the future

Scriban said HealthVault presumes it cannot achieve a critical mass of users if consumers worry the company will license their health data to pharmaceutical companies or others who might want to search and analyze the information.[275] Such practices are known as "data-mining."[276] But, Scriban said:

> [T]here's potentially large research, public health, and commercial potential in the HealthVault population over time. While our privacy policies preclude data mining our users' records, we (and our partners) are thinking hard about ways to approach HealthVault users and solicit their

270. *Id.*

271. HealthVault, Blood Glucose Monitors, http://www.healthvault.com/device/Lifescan-bloodglucose.html (last visited Sept. 22, 2008).

272. HealthVault, Devices That Connect with Health Vault, http://www.healthvault.com/personal/devices.html?type=device (last visited Sept. 22, 2008) (listing hyperlinks to health and fitness monitoring devices such as blood glucose monitors, blood pressure monitors, peak flow meters, and heart-rate monitors that connect to HealthVault records).

273. HealthVault, Use Devices and Gadgets with HealthVault, http://www.healthvault.com/Personal/devices-overview.html (last visited Sept. 22, 2008) (explaining that individuals can upload and store data from their health and fitness devices to their HealthVault record, thus allowing them to share that date with other Web sites).

274. Telephone Interview with George Scriban, *supra* note 17.

275. *Id.*

276. *See, e.g.*, Hatch, *supra* note 31, at 1491 (referring to Metromail Corporation as a "data-mining company" because it "collects more than 900 pieces of information on individual consumers").

participation in things like clinical trials and research studies.[277]

Companies that recruit volunteers to enroll in clinical trials, which test drugs in human beings, may want to invite HealthVault users who have a particular disease to volunteer.[278] Pharmaceutical companies cannot win Food and Drug Administration approval to market a drug for a particular use without proving in clinical trials that it is safe and effective,[279] but finding the right volunteers can be a challenge.[280] Personal health records platforms such as HealthVault have the potential to be very attractive to such companies. For example, Scriban suggested the companies might one day buy key words such as "multiple sclerosis" from Microsoft, allowing them to market clinical trials to users who type those key words into the Live Search Health function available via the HealthVault site.[281]

B. Study Shows Personal Health Record Privacy Statements Generally Are Inadequate

A January 2007 report for the Office of the National Coordinator for Health Information Technology, the office created to pursue an electronic health record by President Bush's executive order, raised concerns about vendors' personal health record privacy policies.[282] The report, which does not name any personal health record vendors, was conducted before HealthVault was officially launched, and examined the privacy policies of thirty vendors.[283] It analyzed thirty-one criteria in categories such as readability, coverage, the gathering of "non-personal data," and "how/if the information is shared."[284] Altarum, the Ann Arbor, Michigan, consultant that conducted the study for the government, distinguished the related concepts of privacy, confidentiality, and security.[285] Privacy refers to "an individual's right to control the acquisition, uses, or disclosures of his

277. E-mail from George Scriban, *supra* note 17.
278. Telephone Interview with George Scriban, *supra* note 17.
279. 21 C.F.R. §§ 314.2, 314.50(d)(5).
280. Ian Urbina, *Panel Suggests Using Inmates in Drug Trials*, N.Y. TIMES, Aug. 13, 2006, at 1 (noting an Institute of Medicine recommendation that would allow more inmates to enroll in drug-testing experiments, which "comes as the biomedical industry is facing a shortage of testing subjects").
281. E-mail from George Scriban, *supra* note 17.
282. ALTARUM INST., REVIEW OF PERSONAL HEALTH RECORD (PHR) SERVICE PROVIDER MARKET: PRIVACY AND SECURITY 1–2 (2007).
283. *Id.* at 2.
284. *Id.* at 4.
285. *Id.* at 2.

or her identifiable health data."[286] Confidentiality is "closely related" and "refers to the obligations of those who receive information to respect the privacy interests of those to whom the data related."[287] Security is the "safeguards or tools used to protect identifiable health data from unwarranted access or disclosure."[288] The report then noted how privacy polices sometimes authorize dissemination of underlying data:

> Privacy therefore is a right that, if broken, has been violated. Security, by comparison, is a product that may be bought and sold under business contracts. Meaningful levels of security are also wholly dependent on the business rules surrounding the confidentiality and privacy of the data they protect. Data can be completely safe from unauthorized breach, but if authorization allows unlimited duplication and dissemination of underlying data then that security has no meaningful interpretation.[289]

In its review of thirty privacy policies, Altarum found that none met more than eighteen of the thirty-one criteria the consultants used to evaluate completeness.[290] Only one vendor policy required consumer's consent before a vendor could share any of the data in a personal health record.[291] None named any business associates of the service providers who "might receive identifiable or de-identified health information;" none provided for notifying the personal health record customer when such data are sold or transferred to a third party; and none said it reveals to the customer what data have been transferred.[292] Only sixteen discussed whether they would share the data with law enforcement; seven discussed research uses of data; and three discussed uses of data in clinical trials.[293] Few personal health record sites detailed how they would safeguard data if users left inactive accounts or the sites merged or failed.[294]

Altarum warned that while service providers may gather non-personal data from users for legitimate reasons, such as to help them

286. *Id.*
287. *Id.*
288. *Id.*
289. *Id.*
290. *Id.* at 6 ("[N]o reviewed privacy policy is even approximately complete.").
291. *Id.* at 7.
292. *Id.* at 13.
293. *Id.* at 9.
294. *Id.* at 9–10.

in administering systems,[295] personal health record vendors may begin selling or leasing user data to increase revenue, if they have not already.[296] One personal health record vendor acknowledges as much: "To defer the costs of bringing you the service, we may at times distribute aggregate information about our members to sponsors, advertisers or business associates, but we will never personally identify you."[297]

The Altarum study points out that most personal health vendors are not covered entities under HIPAA, and they therefore are not bound under that law to de-identify data before sending it to a business associate.[298] "They may find it more cost-effective to send their PHR database to one of their business partners or sponsors under a sell or lease arrangement with the understanding that the third party will extract and use only aggregated or de-identified data."[299] Altarum explains:

> Covered entities under the HIPAA statute are required to protect personal health information, but many PHR service providers are not covered entities and there is no statute or standard that defines PHR service providers' legal responsibilities. Even less clear are the legal restrictions on third parties who are the business partners with the PHR service provider. As a final area lacking clarity, it is entirely unknown what requirements may be placed on offshore or non-U.S. based companies.[300]

VI. STATE ACT COULD ENSURE PERSONAL HEALTH RECORD PRIVACY, THEREBY ENCOURAGING PERSONAL HEALTH RECORD EXPANSION

A. Medical Privacy Violations Have Never Been Unusual

The Hippocratic Oath demonstrates that patients for centuries have feared the harm that can come from the disclosure of medical information.[301] More recently, the Maryland legislature passed the Confidentiality of Medical Records Act amid evidence that the

295. *Id.* at 10.
296. *Id.*
297. *Id.*
298. *Id.* at 11–12.
299. *Id.* at 11.
300. *Id.* at 12.
301. Hatch, *supra* note 31, at 1489.

disclosure of medical records causes harm.[302] An AIDS Partnership Council representative testified before the Senate Economic and Environmental Affairs Committee that a health-care provider had tested another man for HIV without the man's consent.[303] The health-care provider then sent the results, which inaccurately said the man was HIV-positive, directly to the man's employer without his knowledge.[304]

B. Electronic Records Have the Potential to Increase the Frequency and Ease of Medical Privacy Violations

Former Minnesota Attorney General Mike Hatch wrote in 2002 that Americans were concerned about such disclosures and that "[u]nauthorized disclosures or security breaches related to electronic health records have become more frequent."[305] Among other examples, Hatch noted reports that a university researcher accidentally posted the names and psychological evaluations of children on a university home page and that a drug manufacturer revealed the e-mail addresses of individuals with depression, bulimia, and obsessive compulsive disorder.[306]

A September 2003 survey for the Federal Trade Commission noted that a small percentage of identity theft involved people who used pilfered identities to obtain medical care.[307]

In 2005, a California HealthCare Foundation survey revealed more than half of those surveyed said they were concerned about employers potentially using health information "to limit job opportunities."[308] And in 2007, in a piece for the *Journal of Internet Law*, authors Sharona Hoffman and Andy Podgurski noted dangers inherent in the "growing enthusiasm in the United States for computerization of all personal health records".[309]

Electronic health records can be illicitly accessed from anywhere and transmitted across the globe quickly, cheaply, and with little risk

---

302. *See supra* note 220 and accompanying text.
303. *Hearing*, *supra* note 238 (statement of Stuart Harvey).
304. *Id.*
305. Hatch, *supra* note 31, at 1491.
306. *Id.*
307. SYNOVATE, FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT, at 4 (2003), http://www.consumer.gov/idtheft/pdf/synovatereport.pdf.
308. CAL. HEALTHCARE FOUND., NATIONAL CONSUMER HEALTH PRIVACY SURVEY 2005, at 1 (2005).
309. Sharona Hoffman & Andy Podgurski, *Securing the HIPAA Security Rule*, J. INTERNET L., Feb. 2007, at 1, 1.

of detection. Once data is distributed on the Internet, it may become available to anyone who wishes to purchase it, and it cannot be expunged. Accidental or intentional disclosure, corruption, or loss of private health information can, therefore, cause individuals substantial harm. This harm may include serious and life-threatening medical mistakes, duplication of painful medical tests, and violations of privacy.[310]

C. *Personal Health Records Also Promise Benefits*

Personal health records promise significant benefits, including what Hoffman and Podgurski note are the "enhance[ed] processing speed, flexibility, efficiency, and accuracy" of electronic personal health information that can result in better medical care.[311] The Maryland Task Force to Study Electronic Health Records discussed the potential of personal health records, which among other benefits, include doctors' use of them to make decisions "based on a broader set of information than is now available."[312]

D. *The Maryland General Assembly Must Act to Ensure Personal Health Record Benefits Are Realized Quickly and Safely*

There is a flaw in the Task Force's approach of waiting for the personal health records market to develop before suggesting action to clarify the "data ownership rights, privacy obligations, and identification of potential liabilities for all stakeholders."[313] The market for personal health records is likely to develop more rapidly and safely if legislation clearly delineates those rights and obligations.[314]

It may be tempting for the Maryland General Assembly to defer to Congress on the issue, given the obvious advantages to having a single, HIPAA-like law that applies to personal health records in all

310. *Id.* at 1, 6.

311. *Id.* at 1.

312. TASK FORCE FINAL REPORT, *supra* note 10, at 30.

313. *Id.*

314. *See, e.g.*, Nicolas P. Terry, *An eHealth Diptych: The Impact of Privacy Regulation on Medical Error and Malpractice Litigation*, 27 AM. J.L. & MED. 361, 361–62 (2001) (arguing that increasing privacy regulation stimulates electronic health care businesses, which need to ensure privacy and security to gain market share); TASK FORCE FINAL REPORT, *supra* note 10, at 22 ("Mandates imposed through regulations, accreditation standards, or as the result of judicial liability rulings, can push providers to adopt new treatment modalities and patient safety techniques that are based in HIT."); Bernstein et al., *supra* note 195, at 6 ("[A] new legal framework is necessary to promote consumers' access to and use of electronic personal health information.").

jurisdictions.[315] Microsoft, HealthVault's parent company, is among those that favors developing a uniform federal privacy law that spans industries.[316] But by acting, Maryland has an opportunity to encourage the safe, rapid development of the many beneficial uses of personal health records while influencing the direction of federal law. One obvious option would be for the state to expand the Maryland Confidentiality of Medical Records Act to include personal health records. Alternatively, the General Assembly could draw on the work of others who have identified privacy principles to guide employers and others holding personal health records.[317]

One example is the Safe Harbor Privacy Principles the U.S. Department of Commerce issued in July 2000 in response to the European Union's Comprehensive privacy legislation.[318] The European legislation required that "transfers of personal data take place only to non-EU countries that provide an 'adequate' level of privacy protection."[319] Beset by concerns that U.S. businesses would not be in compliance, the Department obtained the European Union's agreement that businesses operating under the Safe Harbor Privacy Principles would qualify as being within a "safe harbor" that presumptively qualified them as compliant.[320] The principles are: (1) notice, requiring an organization to inform individuals about the purposes for which it collects and uses the information about them; (2) choice, requiring organizations to allow individuals to opt out of disclosure to a third party or use of the information incompatible with the purposes for which it was collected; (3) onward transfer, requiring organizations that wish to transfer personal data to third parties to comply with notice and choice, among other things; (4) security, requiring organizations to take reasonable precautions to protect the personal information from loss, misuse, and unauthorized

315. Bernstein, *supra* note 195, at 6.

316. Press Release, Microsoft Corp., Microsoft Advocates Comprehensive Fed. Privacy Legislation (Nov. 3, 2005), *available at* http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx.

317. *See* HEALTH PRIVACY PROJECT, *supra* note 170, at 4 (suggesting, among other principles, that employees control access to and use of an employer-sponsored personal health record); *see also* ALTARUM INST., *supra* note 282, app. C at 1 ("Common to all of these documents . . . are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.").

318. Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000).

319. *Id.* at 45,666–67.

320. *Id.* at 45,667.

access, disclosure, alteration, and destruction; (5) data integrity, requiring personal information to be relevant for the purposes for which it is to be used; (6) access, requiring that individuals about whom data is kept have access to it and the ability to correct, amend, and delete that information; and (7) enforcement.[321]

While private personal health record vendors may argue that they already comply with such principles, the Altarum study shows vendors are not in compliance with even the most fundamental notice principles.[322] Such early problems argue against allowing this emerging industry to police its own practices. A statute packing significant fines or a private right or action "for consumers harmed by an entity's unfair information practices" would be preferable remedies.[323]

The more states that take action, the more likely it is a national policy will emerge. What the Maryland General Assembly should not do is wait. Personal health record Web sites are likely to grow in popularity more quickly if consumers are assured they can rely on statutory protections. Private industry's development of personal health record sites has the potential to finally move health care into the electronic information era. It should not be easier for you or your doctor to download a song or check a bank balance than it is to pull up your latest CAT scan, especially in an emergency.

Juliana Bell

321. *Id.* at 45,667–68.

322. *See supra* Part IV.B.

323. ALTARUM INST., *supra* note 282, app. C at 4. As it takes up the issue, the legislature also should consider the complicated questions health care providers such as Basch have raised: What duty, if any, is created for a physician who reviews a personal health record? What potential liabilities are created, if any, if a physician refuses to look? And what if a physician relies on a personal health record that turns out to be inaccurate? *See supra* notes 180–86 and accompanying text.