William & Mary Law Review

Volume 51 | Issue 6 Article 6

Paging Dr. Google: Personal Health Records and Patient Privacy

Colin P. McCarthy

NOTES

PAGING DR. GOOGLE: PERSONAL HEALTH RECORDS AND PATIENT PRIVACY

TABLE OF CONTENTS

INTRODUCTION

Imagine the following scenario: John, a fifty-three-year-old attorney from Virginia is on vacation in California visiting friends he has not seen since law school. While out at dinner, John appears to have a stroke, and his friends rush him to the nearest hospital. John arrives at the emergency room unresponsive. His friends, knowing nothing of John's medical history, cannot tell the emergency room doctors some vital information that would be helpful for John's diagnosis. John is deteriorating. Without time to wait for lab results, the emergency room doctor administers an appropriate amount of Heparin, a commonly used anticoagulant used to counteract the effects of the stroke.[1] Unfortunately, the treatment has an adverse effect, causing John to bleed internally. John dies shortly after his arrival at the hospital, leaving his friends distraught and his doctors scratching their heads.

What is wrong with this story? Strokes are common medical problems, and modern medicine has advanced to the point where having a stroke is not normally a life-threatening occurrence. John did not die from a stroke; he died from a lack of information. John's friends did not know that two years prior, John had a Mitral valve replacement and had been on prescription Coumadin, a blood thinner, ever since. John could not convey this information to anyone as he was unconscious. The doctor had no access to John's medical records, stored at a hospital in Virginia, which clearly document John's prior procedures and current prescriptions. With this information, John's doctor could have chosen an alternative mode of treatment, and John would have survived.

Doctors and other medical professionals rely on information supplied by the patient and the patient's medical record in making their decisions. A patient's medical record gives a doctor all of the relevant information needed to make an informed and calculated decision about the patient's care and allows the doctor to take into account many factors, including preexisting conditions, prescriptions, changes in diet, and family medical history, among others.

1. WebMD.com, Medical Dictionary: Heparin, http://dictionary.webmd.com/terms/heparin (last visited Mar. 3, 2010).

With this information, a patient's doctor can perform the medical calculus and decide the best course of treatment for the patient.

Recently, a new tool has been introduced that aims to make John's unfortunate story a thing of the past: the personal health record (PHR). A PHR, though a new concept without a uniform definition, has been characterized as "an electronic record of individually identifiable health information on an individual that is drawn from multiple sources and that is managed, shared, and controlled by or for the individual."[2] In essence, a PHR is a medical record owned by the patient, not her doctor or hospital, that can be accessed, usually via the Internet, by the patient, her health care providers, insurance companies, and others to whom the patient authorizes access. Two prominent examples of online PHRs are Google Health[3] and Microsoft HealthVault.[4] The patient may contribute to the PHR by providing information such as prescriptions, allergies, and diet.[5] A patient's health care providers contribute to the PHR by uploading, at the patient's request, copies of her electronic medical records directly into the PHR system.[6] This collaboration is intended to result in a more complete, easy-to-use, and manageable medical record accessible from anywhere with Internet access.

Although PHRs have many potential benefits, there are concerns about the privacy and confidentiality of the data stored within them.[7] This Note will focus on an important question currently in

---

2. PRO(TECH)T Act of 2008, H.R. 6357, 110th Cong. § 300(8) (2008).

3. Google Health, http://www.google.com/health (last visited Mar. 3, 2010).

4. Microsoft HealthVault, http://www.healthvault.com (last visited Mar. 3, 2010).

5. *See, e.g.*, Google Health, About Google Health, http://www.google.com/intl/en-US/health/about/ (last visited Mar. 3, 2010).

6. At the time of this writing, a limited number of providers have active affiliations with Google Health and Microsoft HealthVault. However, Beth Israel Deaconess Medical Center, the teaching and research affiliate of Harvard Medical School, and the Cleveland Clinic are both linked to Google Health. Google Health, Personal Health Services, https://www.google.com/health/directory?cat=importrecords (last visited Mar. 3, 2010). Walgreens Pharmacy, Quest Diagnostics, Medco, and RxAmerica are other major affiliates of Google Health. *Id.* Microsoft HealthVault has partnered with CVS Pharmacy, Beth Israel Deaconess Medical Center, Aetna, and Planned Parenthood, among other providers now offering their patients PHRs. *See* Microsoft HealthVault, Applications Directory, http://www.healthvault.com/personal/websites.html?type=application (last visited Mar. 3, 2010).

7. *See, e.g.*, *Google Online Health Records Service Irks Privacy Watchdogs*, FOXNEWS.COM, May 20, 2008, http://www.foxnews.com/story/0,2933,356663,00.html ("By

debate in the health care and privacy law fields: how the adoption of PHRs will affect the privacy of patients' health information. There is concern that PHR vendors, such as Google and Microsoft, are not governed by the strict privacy and security rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[8] and are held to no other standard in safeguarding patient data stored on their servers.[9] This Note will address and analyze these concerns. Part I will discuss the new age of medical records, in which PHRs will play an important part. Part II will analyze the current state of health care privacy law and its application to PHRs. Part III will set forth the argument that PHRs should be subject to the same or similar privacy regulations as other forms of medical records and will analyze two possible solutions to the problem: (1) amending HIPAA to make PHR vendors comply with its requirements, and (2) enacting a new federal law to promote the use of PHRs while also putting safeguards in place to protect patients' confidential medical data through administrative regulations.

I. THE NEW AGE OF MEDICAL RECORDS

As early as 2001, legal scholars expressed hope for a new age of medical records, easily accessible to both patients and doctors:

> An ideal medical record would be Internet-based, but only available to physicians upon consent of the patient or in a *bona fide* emergency. The record could be electronically segregated into sections allowing various health care providers and others access on a "need to know" basis. The patient should have full "read-only" access to the official record, and only licensed health

transferring records to an external service, patients could unwittingly make it easier for the government, a legal adversary or a marketing concern to obtain private information." (quoting Pam Dixon, Executive Director of the World Privacy Forum)); Posting of Nathan McFeters to ZDNet.com Blog, http://blogs.zdnet.com/security/?p=1166 (May 22, 2008, 08:02 EST) (summarizing other technology bloggers' criticism of Google's privacy practices, including links to other websites that explain how hackers have infiltrated Google's servers and accessed user information, such as Gmail and Google Docs accounts, without permission).

8. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 29 U.S.C. and 42 U.S.C. (2006)); *see also* 45 C.F.R. §§ 144, 146, 160, 162, 164 (2008).

9. *See, e.g.*, Steve Lohr, *Warning on Storage of Health Records*, N.Y. TIMES, Apr. 17, 2008, http://www.nytimes.com/2008/04/17/business/17record.html?_r=1.

> care providers should be able to enter information in the record, to ensure the accuracy of the record. The record could however contain a patient section allowing the patient to enter self-recorded weight and blood pressure, frequency and severity of headaches, and other similar information. Such information could even be entered electronically via biometrics devices.[10]

In 2004, President George W. Bush announced his goal that most Americans would have electronic health records in ten years, envisioning that such a system would be easier for patients to use and understand, while giving medical professionals ready access to vital information about their patients.[11] More recently, in the 2008 presidential campaign, then-candidate Barack Obama focused on health care technology, supporting a move to electronic medical records so that doctors have "easy access to all the necessary information about their patients" and can "reduce costly medical errors."[12] The Department of Health and Human Services (HHS) has stated that health information technology (HIT) can reduce health care costs each year by saving time and reducing duplicative efforts.[13]

---

10. Ronald L. Scott, *Cybermedicine and Virtual Pharmacies*, 103 W. VA. L. REV. 407, 432 (2001).

11. The White House, Transforming Health Care: The President's Health Information Technology Plan, http://georgewbush-whitehouse.archives.gov/infocus/technology/economic_policy200404/chap3.html (last visited Mar. 3, 2010) (site is no longer updated).

12. John Lauerman, *Obama Should Tap Personalized Medicine Tools, Leavitt Says*, BLOOMBERG.COM, Nov. 14, 2008, http://www.bloomberg.com/apps/news?pid=20601124&sid=aHJaVXZ52Fjs&refer=home. Obama spoke on the campaign trail of increasing efficiency and reducing medical errors, promising to invest $50 million over the next five years in health information technology. *See* BarackObama.com, Barack Obama and Joe Biden's Plan To Lower Health Care Costs and Ensure Affordable, Accessible Health Coverage for All, http://www. barackobama.com/pdf/issues/HealthCareFullPlan.pdf (last visited Mar. 3, 2010). The Obama campaign cited a study that projected "up to $77 billion [in] savings ... each year through improvements such as reduced hospital stays, avoidance of duplicative and unnecessary testing, more appropriate drug utilization, and other efficiencies." *Id.*

13. Health Information Technology, http://healthit.hhs.gov/portal/server.pt (last visited Mar. 3, 2010) (site is maintained by U.S. Department of Health and Human Services).

A. Traditional (Paper-Based) Medical Records

From the age of Hippocrates, a patient's medical record has been considered a severely private document.[14] The Supreme Court has recognized a constitutional "right of privacy,"[15] including the right to avoid "disclosure of personal matters,"[16] which has been interpreted to include a person's medical records.[17] Professional ethics rules require physicians to hold information about their patients in confidence.[18] Privacy of medical records is taken seriously for good reason: a patient's medical record includes a wealth of information about the patient, including personal,[19] financial,[20] social,[21] and

14. Greek Medicine, The Hippocratic Oath, http://www.nlm.nih.gov/hmd/greek/greek_oath.html (last visited Mar. 3, 2010) ("Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private.").

15. While first recognized as stemming from the "penumbras" of the Bill of Rights in *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965), the Court later found the right to privacy rooted in the Fourteenth Amendment. *See, e.g.*, Lawrence v. Texas, 539 U.S. 558 (2003); Cruzan v. Mo. Dep't of Health, 497 U.S. 261 (1990).

16. *See* Whalen v. Roe, 429 U.S. 589, 599 (1977) (protecting "the individual interest in avoiding disclosure of personal matters").

17. *See, e.g.*, Doe v. Delie, 257 F.3d 309, 315 (3d Cir. 2001) (quoting United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980)) (recognizing a long-standing right to privacy of medical records); Doe v. Se. Pa. Transp. Auth., 72 F.3d 1133, 1138 (3d Cir. 1995) (extending the right to privacy to a patient's prescription records); *Westinghouse Elec. Corp.*, 638 F.2d at 577 ("There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection.").

18. COUNCIL ON ETHICAL & JUDICIAL AFFAIRS, CODE OF MEDICAL ETHICS OF THE AMERICAN MEDICAL ASSOCIATION 136-80 (Am. Med. Ass'n 2007) [hereinafter CODE OF MEDICAL ETHICS].

19. Personal data usually includes the patient's "name, birth date, sex, marital status, next of kin, [and] occupation." WILLIAM H. ROACH ET AL., MEDICAL RECORDS AND THE LAW 32 (4th ed. 2006).

20. For billing and insurance purposes, a patient's medical record contains his or her insurance policy numbers and Medicare or Medicaid numbers. *Id.*

21. Providers also record social data such as "race[,] ... ethnic background, family relationships, community activities, and lifestyle." *Id.*

medical data.[22] A patient's medical record will also include administrative information such as consent and authorization forms.[23]

Traditionally, all of this data would accumulate over years in a patient's paper medical record, resulting in stacks of manila folders in a file cabinet at the patient's doctor's office, hospital, or other health care facility. With hundreds and thousands of different patients, all with their own lengthy records, storage and security of this vital information poses a serious consideration for health care facilities.[24] On one hand, a patient's record needs to be easily accessed by their provider; on the other, it must be secured from unauthorized access.[25] Although storing medical records in digital form does not completely eliminate the problem of unauthorized access,[26] electronic medical records may be monitored and audited more easily than paper records.

---

22. Most importantly, a patient's medical record contains an extensive history of the patient's medical procedures and problems, including: complaints and symptoms; medical and family histories; physical examination results; prior treatments, diagnoses, physician orders, therapy records, clinical observations, progress notes, nursing notes; and reports generated during the patient's prior treatment, including pathology tests, operations, radiology and nuclear medicine examinations, and anesthesia records. *Id.*

23. *Id.*

24. According to the American Hospital Association, in 2000, hospitals planned to spend $22.5 billion over five years to ensure compliance with federal and state privacy laws. *See* Dan Coate & Keith MacDonald, *Projecting the Budget Impacts of HIPAA*, HEALTHCARE FIN. MGMT., Feb. 2002, at 43, 43.

25. It is not uncommon for medical records to fall into the wrong hands, including those of an employee of the health care provider itself. *See, e.g.*, *20 Hospital Workers Fired for Viewing Collier's Medical Records*, NEWS4JAX.COM, Oct. 31, 2008, http://www.news4jax.com/print/17859733/detail.html (reporting the firing of twenty hospital employees for accessing NFL player Richard Collier's medical record without authorization during Collier's stay in Shands Jacksonville Hospital after being shot fourteen times); Charles Ornstein, *Ex-worker Indicted in Celebrity Patient Leaks*, L.A. TIMES, Apr. 30, 2008, at A1, *available at* http://articles.latimes.com/2008/apr/30/local/me-ucla30 (describing the leak of celebrity Farrah Fawcett's cancer treatment by a UCLA Medical Center employee, who allegedly profited $4,600 by selling the information to *The Enquirer*).

26. *See* Edvige Jean-Francois, *Stolen Laptop Contains Personal Info of 2,500 Patients*, CNN.COM, Mar. 25, 2008, http://edition.cnn.com/2008/US/03/25/stolen.laptop/index.html (detailing the theft of a government laptop containing the unencrypted health records of 2500 patients of the National Heart, Lung, and Blood Institute).

B. Electronic Medical Records, Personal Health Records, and Health Information Exchanges

1. Electronic Medical Records

In recent years, health care providers have been moving away from traditional paper-based medical records to electronic medical records (EMRs)[27]—medical records created and used by medical providers in electronic form.[28] An EMR contains all of the information a traditional paper-based medical record does but without the problems inherent in a paper-based system, such as illegible physician handwriting, insufficient physical storage space, and lack of security. Each health care provider maintains its own EMRs—physician's offices maintain their EMRs, hospitals maintain their EMRs, and so on. Herein lies the inadequacy of stand-alone EMRs: they do not follow the patient. In John's case, his doctors had no access to the EMR on file with his hospital at home in Virginia—the EMR that clearly and prominently noted his prescriptions and other information that would have saved John's life.

EMRs generally incorporate computerized provider order entry systems (CPOEs), which allow physicians to order medications with greater ease and accuracy than before by "only accepting typed orders in a standard and complete format."[29] The CPOE system may link directly to the hospital's pharmacy where pharmacists can quickly dispense the correct amount of medication, discover discrepancies in physician orders, and avoid costly medical errors.[30] EMRs

---

27. *See* Paul C. Tang et al., *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, 13 J. AM. MED. INFORMATICS ASS'N 121, 121 (2006) ("Over the past several years, there has been a remarkable upsurge in activity promoting the adoption of electronic health records (EHRs). All levels of government—federal, state, regional, and local—as well as the private sector, have encouraged EHR adoption.").

28. Kirk J. Nahra, *How Health Information Exchange Is Driving a New Health Care Privacy Debate*, 7 PRIVACY & SEC. L. REP. 795 (2008).

29. Rainu Kaushal & David W. Bates, *Computerized Physician Order Entry (CPOE) with Clinical Decision Support Systems (CDSSs)*, *in* MAKING HEALTH CARE SAFER: A CRITICAL ANALYSIS OF PATIENT SAFETY PRACTICES 59, 59 (Kaveh G. Shojania et al. eds., 2001), *available at* http://www.ahrq.gov/clinic/ptsafety/chap6.htm.

30. *See* Anne Bobb et al., *Computerized Physician Order Entry and Online Decision Support*, 11 ACAD. EMERGENCY MED. 1135, 1135 (2004); Ceci Connolly, *Cedars-Sinai Doctors Cling to Pen and Paper*, WASH. POST, Mar. 21, 2005, at A01, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A52384-2005Mar20 (describing an instance in which a CPOE

have great benefits in that they may reduce errors caused by misreading a physician's orders or misfiled paperwork in a large paper file, but they are limited by their inoperability with other providers.

2. Personal Health Records

Personal health records (PHRs) act as "a mechanism for consumers to gather, store and disseminate their own health care information."[31] The Department for Health and Human Services defines a PHR as "an electronic file or record of [a patient's] health information and recent services, such as ... allergies, medications, and doctor or hospital visits that can be stored in one place, and then shared with others, as [the patient] see[s] fit."[32]

PHRs offer patients an opportunity to create an online health profile, including basic biographical data such as height, weight, and age, as well as more detailed health data such as current prescriptions, past procedures, conditions, immunizations, and allergies.[33] This allows the patient to have all of her relevant health care information stored in one place, accessible from anywhere with an Internet connection.[34] What makes these PHRs special, however, is that they can interact with the patient's health care provider.[35] If the patient's doctor, pharmacy, or hospital has become affiliated with a PHR provider, the patient can choose to upload her medical records directly into the PHR.[36] Until now, patients could request a copy of her medical records from their health care providers but have not had the opportunity to control them in the way that PHRs offer. PHRs allow patients to play a more active role in their health care. Although it is unlikely that all patients will take the initiative to keep their PHRs up-to-date, those with chronic illnesses will

---

system alerted a physician that he had entered an order for ten times the proper dosage of a drug).

31. Nahra, *supra* note 28, at 796.

32. Medicare, Personal Health Records (PHR), http://www.medicare.gov/PHR/Overview.asp (last visited Mar. 3, 2010).

33. *See* Google Health, *supra* note 5.

34. *Id.*

35. *Id.*

36. For examples of the current affiliates with PHR systems, see *supra* note 6.

likely benefit from an increased ability to track their diseases.[37] These patients may also benefit from using home monitoring devices such as blood pressure monitors, scales, and other instruments that link to their PHRs.[38]

Recall the scenario described above. If John had a PHR affiliated with his health care provider, the emergency room doctors would have had all of John's prior medical records at their disposal,[39] and would have been able to treat John with a lower dose of Heparin—thus, avoiding a fatal medication error. This is one of the primary goals of PHRs—to decrease medication errors and other problems that arise from a lack of information about the patient's medical history.

3. Health Information Exchanges

The interplay between one provider's EMR and another provider's EMR, or a provider's EMR and a patient's PHR, has been characterized as a health information exchange (HIE).[40] HIEs facilitate communication between providers and patients to form a complete medical record of the patient, across facilities and state and regional boundaries. "The goal of these exchanges is to improve medical outcomes and reduce medical errors, for example, by identifying a potential drug interaction with the drug provided by the pharmacy."[41] The idea behind a HIE is simple: share a patient's EMR from one facility with another facility, and vice versa. This allows a patient to visit different facilities without having to request a copy of her medical records be sent each time. In practice, however, these arrangements are difficult to implement on a large scale and have only resulted in regional networks, known as regional health information organizations.[42]

---

37. *See* Tang et al., *supra* note 27, at 123 ("Patients with chronic illnesses will be able to track their diseases in conjunction with their providers, promoting earlier interventions when they encounter a deviation or problem.").

38. *See id.*

39. Ideally, John's surgeons could simply input his name and Social Security number—or other identifier—into their EMR system, and it would find John's online PHR and upload it to their local system.

40. *See* Nahra, *supra* note 28.

41. *Id.*

42. *See id.*

C. Benefits and Potential Problems of Personal Health Records

As discussed above, PHRs provide various benefits for patients and providers alike. First and foremost, they allow for an increased quality of care—with more complete information, doctors can provide better care. Second, having a patient's health information stored in a central, Internet-accessible record allows providers from all over the world to access the patient's medical information, cutting the administrative and logistical costs of copying and transferring a medical record from one provider to another.[43] Third, PHRs give patients more control over their health information, empowering them to monitor their health and learn more about staying healthy.[44]

Despite the benefits of PHRs, some see even greater potential problems arising from the proliferation of these new services. First, there is concern that relinquishing control over a patient's records to the patient may lead to inaccurate and incomprehensive records, as patients may redact vital information that they do not wish to share with their doctor, even if it is relevant to their care and treatment.[45] Others raise concerns of interoperability and argue that the cost to providers to join these new systems will be too high to be implemented nationally.[46]

A main concern, and the central topic of this Note, is the privacy, or lack thereof, of data stored in PHRs. PHR vendors, such as Google Health and Microsoft HealthVault, are not subject to the strict privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA) because they are not "covered entities."[47] How, or if, PHRs will be subject to federal privacy

---

43. *See* Linda A. Malek & Jay D. Meisel, *Electronic and Personal Health Records: The Risks and Benefits for Providers*, 17 HEALTH L. REP. 555 (2008).

44. *See* Tang et al., *supra* note 27, at 123.

45. Malek & Meisel, *supra* note 43.

46. *Id.*

47. *See* Google Health, Google Health and HIPAA, http://www.google.com/intl/en/health/hipaa.html (last visited Mar. 3, 2010) ("Unlike a doctor or health plan, Google Health is not regulated by the Health Insurance Portability and Accountability Act (HIPAA)."); Microsoft HealthVault, Microsoft HealthVault Account Service Agreement, https://account.healthvault.com/help.aspx?topicid=ServiceAgreement (last visited Mar. 3, 2010) ("The Service does not hold designated record sets as defined under the U.S. Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder (HIPAA), nor medical records as defined under state law."); *infra* Part II.B.

regulations remains to be seen. This Note will analyze different proposals in Part III, but before such a discussion, some background in the current state of health care privacy law is necessary.

II. THE CURRENT STATE OF HEALTH CARE PRIVACY LAW

As discussed above, a patient's medical record is a complete account of that patient's medical history and includes personal, social, and financial information.[48] Before the passage of HIPAA, medical records were not subject to specific privacy requirements and were only protected by the constitutional or common law right to privacy, which was overbroad and insufficient to protect the sanctity of medical records.[49]

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

1. What is HIPAA?

The Health Insurance Portability and Accountability Act was enacted in 1996 "to improve the portability and continuity of health insurance coverage, to combat waste, fraud, and abuse in health care, to promote the use of medical savings accounts, to improve access to long term care, and to simplify the administration of health insurance."[50] In Title II of HIPAA, Congress enabled the HHS to promulgate regulations regarding the privacy and security standards to apply to protected health information (PHI).[51] PHI is defined by the rules as individually identifiable health information that is transmitted by electronic media, maintained in electronic form, or transmitted in any other form or medium.[52]

HIPAA applies to "covered entities," defined as health plans, health care clearinghouses, or health care providers that transmit

48. *See supra* notes 19-22 and accompanying text.

49. *See* ROACH ET AL., *supra* note 19, at 115.

50. Gina Marie Stevens, *A Brief Summary of the HIPAA Medical Privacy Rule*, *in* THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA): OVERVIEW AND ANALYSES 91, 93 (Chaikind et al. eds., 2004).

51. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, tit. II, § 201(a), 110 Stat. 1991 (codified at 42 U.S.C. § 1320a-7c (2006)).

52. 45 C.F.R. § 164.103 (2008).

health information in electronic form in connection with health care transactions.[53] A health plan can be a group health plan, health insurance provider, health maintenance organization (HMO), or other provider of public or private insurance coverage.[54] A health care clearinghouse is a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that facilitate transactions between health care providers and insurance companies.[55]

A health care provider is a provider of medical, health, or other services, or "any other person or organization who furnishes, bills, or is paid for health care in the normal course of business."[56] This includes such professionals as dentists, doctors, therapists, and nurses, and organizations such as hospitals, clinics, and other health care institutions.[57]

Covered entities, mostly health care providers and payors, must comply with administrative rules promulgated by HHS, most notably the Privacy Rule and the Security Rule.

2. The Privacy Rule

The Privacy Rule regulates how covered entities handle PHI.[58] The Privacy Rule states that a covered entity may not disclose a patient's PHI without authorization unless it is used for carrying out treatment, payment, or health care operations.[59] Disclosure, under the Privacy Rule, occurs when PHI is "released, transferred, or otherwise revealed to persons *outside* the covered entity that

53. 45 C.F.R. § 160.102.

54. *See* 45 C.F.R. § 160.103.

55. *See id.* ("Health care clearinghouse[s] ... [perform] either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.").

56. *Id.*

57. JUNE M. SULLIVAN, HIPAA: A PRACTICAL GUIDE TO THE PRIVACY AND SECURITY OF HEALTH DATA 4 (2004).

58. ROACH ET AL., *supra* note 19, at 117.

59. 45 C.F.R. § 164.502(a)(1).

holds the PHI."[60] When disclosure is permitted, covered entities must adhere to the Minimum Necessary Rule: covered entities must limit the use or disclosure to the minimum amount necessary to accomplish the intended purpose of the use or disclosure.[61]

When a covered entity shares PHI with another covered entity, it must take reasonable precautions to limit access to those who need access in order "to accomplish their valid job responsibilities related to [treatment, payment, and operations]."[62] This means that if an individual at a hospital is not associated with the treatment, payment, or other legitimate operations regarding a patient, that individual should not have access to the patient's PHI. This Privacy Rule is especially important in hospitals that serve celebrities, politicians, and others whose PHI may stir the curiosity of hospital employees.[63]

3. The Security Rule

The Security Rule only applies to electronic PHI.[64] The Security Rule establishes standards for physical protection of electronic PHI, both while stored and transferred.[65] Under the Security Rule, covered entities must comply with four security requirements: (1) "[e]nsure the confidentiality, integrity, and availability of all [PHI] that the covered entity creates, receives, maintains, or transmits"; (2) "[p]rotect against reasonably anticipated threats or hazards to the security or integrity" of PHI; (3) "[p]rotect against reasonably anticipated uses or disclosures" of PHI in violation of the Security Rule; and (4) "[e]nsure compliance with the Security Rule" by its employees.[66] The requirements are broad and sweeping, and the regulations offer covered entities little guidance on meaning.[67]

---

60. SULLIVAN, *supra* note 57, at 6.

61. 45 C.F.R. § 164.502(b)(1); ROACH ET AL., *supra* note 19, at 146.

62. KEVIN BEAVER & REBECCA HEROLD, THE PRACTICAL GUIDE TO HIPAA PRIVACY AND SECURITY COMPLIANCE 50-51 (2004).

63. See *supra* note 25 for examples of how patients' PHI has been mishandled by hospital employees.

64. 45 C.F.R. § 164.302.

65. ROACH ET AL., *supra* note 19, at 119.

66. *Id.* at 119-20.

67. *Id.* at 120.

The Security Rule also establishes certain administrative safeguards that covered entities must implement in order to be in compliance.[68] First, the Security Rule requires that covered entities develop a "security management process" to "prevent, detect, contain, and correct security violations."[69] Covered entities must also appoint an official within their organization to be responsible for compliance with the Security Rule.[70] Many times, an in-house counsel or technology officer fills this role. Covered entities must also develop policies, defined as "workforce security" by the Security Rule, regarding the access rights of different employees within their organization.[71] In addition to determining who can access which data, covered entities must regularly train their employees about the Security Rule's requirements.[72] The Security Rule mandates other administrative safeguards, such as accounting of security breaches,[73] planning for unexpected events,[74] and continually evaluating the covered entity's security policies.[75]

Covered entities must also adhere to certain physical security safeguards set forth in the Privacy Rule.[76] Covered entities must develop policies to protect PHI from unauthorized access by controlling physical access to the information systems and facilities that house those systems.[77] More specifically, covered entities must control access and user privileges at individual workstations or computer stations where PHI is accessible in electronic form.[78] Part of this control includes technical safeguards, including user identifications, to identify and audit access.[79]

As can be seen from the preceding summary of the HIPAA Security Rule, covered entities, such as hospitals, are under strict regulation in regard to their duty to protect PHI. Not only must these entities develop policies to ensure compliance with the Rules,

68. *Id.* at 461.
69. 45 C.F.R. § 164.308(a)(1); ROACH ET AL., *supra* note 19, at 462.
70. 45 C.F.R. § 164.308(a)(2).
71. *Id.* § 164.308(a)(3).
72. *Id.* § 164.308(a)(5)(i).
73. *Id.* § 164.308(a)(6).
74. *Id.* § 164.308(a)(7).
75. *Id.* § 164.308(a)(8).
76. *Id.* § 164.310.
77. *Id.* § 164.310(a)(1).
78. *Id.* § 164.310(b)-(c).
79. *Id.* § 164.310(2)(iii).

they must continually evaluate and update their policies as necessary to ensure compliance. As new technology emerges, covered entities must edit policies to ensure that only those individuals with a legitimate interest have access to a patient's PHI.

B. HIPAA and PHR Vendors

PHR vendors, such as Google Health and Microsoft HealthVault, are not considered "covered entities" under HIPAA because they are not health plans, health care providers, or health care clearinghouses under the definitions of HIPAA.[80] Accordingly, there is no federal health care privacy law that governs how they store, transmit, or otherwise use PHI. Thus, there exists a gap in the traditional HIPAA structure, a gap that has emerged because technology has moved faster than regulation. That gap should be closed. According to Kirk Nahra, "Most of the advisory groups that have opined on this topic have recommended that either the HIPAA rules be extended to these participants in health information exchanges and personal health records, or that new rules be created for these entities."[81]

III. WHAT SHOULD BE DONE TO PROTECT PHR PRIVACY?

A. Why Should PHRs Be Afforded Privacy Protection or Regulation?

Before conducting an analysis of how to regulate PHR privacy, the need for such protection must be defended. First, the widespread implementation of PHRs is important for the health care industry as it moves into the twenty-first century. Patients have become more involved in their own health care, often consulting the Internet before arranging an appointment with their physicians.[82] PHRs give patients the ability to catalog their symptoms and other

80. *See supra* Part II.A.1.

81. Nahra, *supra* note 28.

82. *See Web Sites May Save You a Trip to the Doctor*, CBS13.com, Jan. 29, 2009, http://cbs13.com/health/Web.sites.medical.2.921282.html (recommending three websites—MedicineNet.com, WebMD.com, and MayoClinic.com—as quality sources of online medical information).

vital information for use in their own medical searches, as well as for use by their physicians.[83]

PHR vendors should be subject to some privacy regulation because of the sensitive and personal nature of the data they hold. The contents of a patient's medical record are inherently private and personal; unauthorized disclosure of such information is a breach of the patient's constitutional right to privacy.[84] In *Griswold v. Connecticut*, the Supreme Court found a right to privacy in the "emanations" of the "penumbras" of the Bill of Rights.[85] This fundamental right to privacy was quickly extended to medical records, for they document the very information the "zone of privacy" was found to protect.[86] Additionally, physicians are held to a professional standard of confidentiality,[87] and various statutory privileges protect the physician-patient relationship.[88]

The problem with the lack of regulation of PHR vendors is that, unlike HIPAA, there are no powerful enforcement mechanisms to ensure that patient data is kept secure and not disclosed without authorization from the patient. Furthermore, PHRs have a unique profit structure compared to health care providers—Google and many other online services companies rely on the sale of advertising for a large share of their revenue.[89] This profit motive raises fears that patient data stored in PHRs could be sold to advertisers in

---

83. *See supra* Part I.C.

84. *See supra* Part I.A.

85. 381 U.S. 479, 484 (1965) (finding that a "zone of privacy" was created by the First, Third, Fourth, Fifth, and Ninth Amendments); *see also supra* note 15.

86. *See* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) ("There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection.").

87. *See* CODE OF MEDICAL ETHICS, *supra* note 18, at 136.

88. The Federal Rules of Evidence do not expressly recognize the physician-patient privilege, though, in some cases, they incorporate state privilege law which does. *See* FED. R. EVID. 501. For examples of state physician-patient privilege statutes, see CAL. EVID. CODE § 994 (2008); OHIO REV. CODE ANN. § 2317.02(B) (2008); VA. CODE ANN. § 8.01-399 (2008). *But see, e.g.*, Northwestern Memorial Hosp. v. Ashcroft, 369 F.3d 923, 926 (7th Cir. 2004) ("[T]here is no federal common law physician-patient privilege.").

89. Internet advertising revenues in the United States totaled $21.2 billion in 2007. INTERACTIVE ADVER. BUREAU, IAB INTERNET ADVERTISING REVENUE REPORT 3 (2008), http://www.iab.net/media/file/IAB_PwC_2007_full_year.pdf.

efforts to target online advertisements to users with certain ailments.[90]

Opponents of PHR regulation may assert that, because PHRs are consumer-based and voluntary, online service companies should not be expected to comply with strict privacy regulations such as HIPAA. In other words, consumers choosing to store their private health care information on a third party's server accept and understand the common Internet security risks—for example, their information may be hacked into, disclosed, or otherwise accessed without consent.

Such advocates would likely support the Federal Trade Commission's (FTC) method of Internet enforcement: simply enforce PHR vendors' privacy policies against them.[91] If a PHR vendor violates its privacy policy, then it may be subject to suit from the FTC on behalf of the injured party and will likely be forced to settle the suit and comply with FTC regulations or face serious fines.[92]

B. The Ineffectiveness of FTC Enforcement of PHR Vendor Privacy Policies

As stated above, one option for privacy enforcement of PHRs currently exists: the FTC could enforce online PHR vendors' privacy policies through section 5 of the FTC Act,[93] which empowers the FTC to "enforce the promises in privacy statements, including promises about the security of consumers' personal information."[94] The FTC uses this authority to hold companies liable for breaches of privacy in violation of their online privacy policies.[95] Google

90. *See* Posting of Karama Neal to Bioethics Forum, http://www.thehastingscenter.org/Bioethicsforum/Post.aspx?id=1528 (May 22, 2008) ("The real concern with Google Health is that it makes sales pitches from pharmaceutical companies part and parcel of medical decision-making.").

91. *See infra* Part III.B.

92. *See infra* Part III.B.

93. 15 U.S.C. § 45 (2006).

94. Federal Trade Commission, Enforcing Privacy Promises: Section 5 of the FTC Act, http://www.ftc.gov/privacy/privacyinitiatives/promises.html (last visited Mar. 3, 2010).

95. *See* Federal Trade Commission, Guidance Software Inc. Settles FTC Charges (Nov. 16, 2006), http://www.ftc.gov/opa/2006/11/guidance.shtm (describing the FTC's settlement with a software company that "fail[ed] to take reasonable security measures to protect sensitive consumer data" in contradiction with "security promises made on its Web site"); Federal Trade Commission, Online Pharmacies Settle FTC Charges (July 12, 2000),

Health's Privacy Policy asserts that each user is "in control" of her data.[96] By signing up for Google Health, however, a user also assents to Google's general Privacy Policy,[97] which seems to include a loophole. Google may disclose user data without the user's consent in certain circumstances, including fraud investigations.[98] So, if an insurance company calls Google and asks for access to a user's records to help with an insurance fraud investigation, then Google's Privacy Policy indicates that Google could share the user's PHI without violating its policies. This is a major crack in the system and is the result of a lack of clear rules for vendors of online PHRs. Though the FTC has authority to enforce companies' privacy policies, such a system is inherently flawed: the company gets to write the rules to which it must conform, and there are no particular requirements that a privacy policy needs to meet.

In contrast, HIPAA requires health care providers and other covered entities to take substantial precautions and implement various safeguards to actively protect PHI.[99] Though covered entities have discretion as to how to best implement privacy and security policies in their facilities, they must meet the strict requirements of the Privacy and Security Rules.[100] Instead of simply adhering to a privacy policy, HIPAA mandates that covered entities take constant concern over privacy and security by continually auditing, monitoring, and augmenting security when necessary.[101]

The FTC's passive regulatory scheme is not sufficient given the highly personal nature of a patient's health care data. A patient's

---

http://www.ftc.gov/opa/2000/07/iog.shtm (detailing allegations and settlement of online pharmacy group's false statements in its privacy and security policy).

96. Google Health, Google Health Privacy Policy, http://www.google.com/intl/en-US/health/privacy.html (last visited Mar. 3, 2010).

97. *Id.*

98. Google, Privacy Policy, http://www.google.com/privacypolicy.html (last visited Mar. 3, 2010) [hereinafter Google Privacy Policy] (Google reserves the right to disclose user data when it has "a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of Google, its users or the public as required or permitted by law").

99. *See supra* Part II.A.

100. *See supra* Part II.A.

101. *See supra* notes 72-75 and accompanying text.

PHR would ideally contain every datum of her medical life—a complete picture of her physical, mental, and emotional status—the very essence of who that person is. This, the most personal of information, is for the patient's—and authorized parties'—eyes only. HIPAA addresses these considerations by creating a strict framework of regulation that covered entities must comply with.[102] Such protection, whether in the form of HIPAA or a separate federal statute and regulations, must be afforded to information stored in PHRs—it is the same information that covered entities must protect, just in a different place.

C. Amend HIPAA To Include PHR Vendors as Covered Entities

Another option to regulate PHR vendors is to amend the definition of a covered entity under HIPAA including PHR vendors and other stewards of PHI. PHR vendors would be subject to the Privacy and Security Rules of HIPAA discussed in Part II.A. This option would ensure that PHI stored on Google or Microsoft's servers, for example, would be afforded the same safeguards as if it was stored on a hospital's server, thus quelling patients' concerns about making medical records available online.

Simply adding PHR vendors to the list of covered entities under HIPAA, however, would not be an adequate way to deal with the problem of PHR privacy. HIPAA was enacted in 1996, before legislators envisioned the idea of a PHR stored "in the cloud."[103] HIPAA's regulations are broad and sweeping.[104] They do not specify exact security requirements, such as what type of encryption is necessary for electronic medical records, or other more technical requirements, which would aid PHR vendors in establishing privacy policies.[105]

---

102. *See supra* Part II.A.

103. Storing information online instead of on a physical drive is often referred to as storing information "in the cloud." *See* Steve Lohr, *Google and I.B.M. Join in 'Cloud Computing' Research*, N.Y. TIMES, Oct. 8, 2007, http://www.nytimes.com/2007/10/08/technology/08cloud.html. Thus, services like web-based email and word processing are referred to as "cloud computing." *Id.*

104. *See supra* Part II.A.

105. *See supra* Part II.A. The Privacy and Security Rules require covered entities to put procedural safeguards in place to protect PHI but offer little guidance on how to implement the regulations. *See supra* Part II.A.

Still, the general rules of HIPAA should apply to PHR vendors: disclosure of a patient's PHI should not occur without that patient's prior consent, unless there is a legitimate health care purpose.[106] More specific technologically informed rules in the form of new federal laws and regulations should also be promulgated to cover PHR vendors.

D. New Federal Law To Govern PHR Privacy and Security

Two proposed laws in the 110th Congress addressed PHRs and the privacy concerns inherent in them, but neither set forth any proposed rules to govern how PHR data should be protected. The Wired for Health Care Quality Act[107] sought "[t]o enhance the adoption of a nationwide interoperable health information technology system and to improve the quality and reduce the costs of health care in the United States."[108] The bill did not specifically address what the privacy rules would look like for PHRs, but it required the Secretary of Health and Human Services "to develop 'recommendations for privacy and security protections for personal health records.'"[109] Similarly, the proposed PRO(TECH)T Act of 2008[110] required the HHS Secretary, in conjunction with the FTC, to submit recommendations to Congress "to identify requirements relating to security, privacy, and notification in the case of a breach of security or privacy ... that should be applied to vendors of personal health records and to third party service providers that such vendors make available to individuals with personal health records."[111]

One of these recommendations—the requirement that a PHR user be notified of a breach of her data—was adopted by the 111th Congress as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act,[112] passed as part of

106. *See supra* note 62 and accompanying text (discussing disclosure of PHI for "treatment, payment, and operations").

107. S. 1693, 110th Cong. (2007).

108. *Id.*

109. Kirk J. Nahra, *Are Troublesome HIPAA Changes on the Way?*, 2008 PRIVACY & DATA SEC. L.J. 573, 575.

110. H.R. 6357, 110th Cong. (2008).

111. *Id.* § 314(1).

112. H.R. 1-112, 111th Cong. (2009).

the American Recovery and Reinvestment Act of 2009.[113] HHS recently promulgated an Interim Final Rule that requires PHR vendors to comply with notification requirements in cases of breach.[114] This is an important step, but the new regulation does not require PHR vendors to adhere to any standardized privacy or security standards, nor does it prohibit the sale of PHI by PHR vendors.[115] The HITECH Act requires HHS to conduct a study to determine what, if any, additional privacy and security requirements should be applied to PHR vendors.[116] The HHS Secretary, charged with the responsibility of conducting this study, should rely on a publication of the HHS Office of the National Coordinator for Health Information Technology, which proposes eight principles to act as guidelines in the exchange of electronic health information.[117]

These principles include: (1) Individual Access; (2) Correction; (3) Openness and Transparency; (4) Individual Choice; (5) Collection, Use, and Disclosure Limitation; (6) Data Quality and Integrity; (7) Safeguards; and (8) Accountability.[118] This report sets guidelines that "are expected to guide the actions of all health care-related persons and entities that participate in a network for the purpose of electronic exchange of individually identifiable health information."[119] Although these guidelines are helpful in formulating policy, they do not have the binding effect of law.

The most important guideline, which should be implemented into law through rule or regulation, is that "[i]ndividually identifiable health information should be protected with reasonable administra-

113. H.R. 1-1, 111th Cong. (2009).

114. Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009).

115. *See* Jordan Cohen, *HIPAA, the HITECH Act, and How Google May Still Be Able To Distribute, and Profit From, Your Personal Health Info*, HEALTHREFORMWATCH.COM, Aug. 6, 2009, http://www.healthreformwatch.com/2009/08/06/hipaa-the-hitech-act-and-how-google-may-still-be-able-to-distribute-and-profit-from-your-personal-health-info (describing the HITECH Act's failure to extend HIPAA's Privacy and Security Rules to PHRs and its omission of PHR vendors from those prohibited from receiving remuneration in exchange for PHI).

116. *See* H.R. 1-163, 111th Cong. (2009).

117. OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., NATIONWIDE PRIVACY AND SECURITY FRAMEWORK FOR ELECTRONIC EXCHANGE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (2008), *available at* http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf.

118. *Id.* at 6-10.

119. *Id.* at 6.

tive, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure."[120] This standard is essentially the same as the standard required by HIPAA,[121] but extended to PHR vendors. What constitutes a "reasonable" safeguard must be determined by consulting technology and health care industry experts, and it must be a flexible standard that can evolve as technology progresses. Currently, the industry-standard technical safeguards for encrypting sensitive online data is 128-bit secure socket layer encryption, which is used by online banking services.[122]

Additionally, the Secretary must consider the public policy behind promoting the use of PHRs, the barrier imposed on the widespread use of PHRs by the lack of privacy protection, the sensitive nature of the data contained in PHRs, and the need for new, innovative rules that take into account the fact that medical data stored in PHRs is in "the cloud."

First, there is strong public policy behind promoting the use of PHRs. Patients will be empowered by owning their health care information, especially those managing chronic illnesses and conditions.[123] Health care providers, with more complete data, will be able to make more well-informed treatment decisions, particularly when treating a new patient or a trauma patient with no prior history at the facility.[124] Having one medical record that follows the patient from provider to provider will also reduce health care costs and avoid duplication and unnecessary tests.[125] As Representative John Dingell said regarding the introduction of the PRO(TECH)T Act, "Your grocery store can immediately determine what brand of

120. *Id.* at 9.

121. *See supra* Part II.A.

122. *See, e.g.*, Bank of America, Online Banking Security and Technical Frequently Asked Questions, http://www.bankofamerica.com/onlinebanking/index.cfm?template=faq_security&statecheck=VA#ssl (last visited Mar. 3, 2010). Bank of America explains encryption as "the scrambling of information for transmission back and forth between two points." *Id.* All information a user inputs after logging into the website and all the information Bank of America sends from its servers is scrambled and can only be decoded by the end user's browser using an encryption key. *Id.*

123. *See supra* Part I.B.2.

124. *See supra* Part I.B.2.

125. *See* Lohr, *supra* note 9; RAND Corp., Health Information Technology: Can HIT Lower Costs and Improve Quality?, http://www.rand.org/pubs/research_briefs/RB9136/index1.html (last visited Mar. 3, 2010).

cereal you bought last year, but your cardiologist cannot quickly find what prescriptions your family doctor wrote for you last week."[126]

Yet patients may be reluctant to move their records into web-based PHRs without some assurance of privacy. Google and Microsoft have other obligations, such as generating ad revenue, that may conflict with their promises of privacy through their privacy policies.[127] Recent studies have shown that consumers are concerned about the privacy of their PHI and are less confident in its privacy when stored in electronic format rather than traditional paper format.[128]

The sensitive nature of patients' medical information stored in PHRs demands stalwart protection.[129] Like a mail courier delivering important documents, PHR vendors should securely transport PHI through cyberspace without compromising its confidentiality. The doctor-patient relationship affords PHI the benefit of the strict rules of HIPAA.[130] Instead of a focus on *who* stores the data, which is how HIPAA approaches the issue, the focus should be on the data itself—its personal nature warrants protection, regardless of storage medium.[131] Federal courts recognized the privacy of medical data,

---

126. Comm. on Energy and Commerce, PRO(TECH)T Act Would Improve Exchange of Health Information & Safeguard Patient Privacy (July 22, 2008), http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1215&catid=17:benefits&Itemid=58.

127. Google's unofficial service motto, "Don't be evil," does not guarantee that the company will not decide to change its privacy policy in the future. *See* Google Investor Relations, Google Code of Conduct, http://investor.google.com/conduct.html (last visited Mar. 3, 2010); *see also* Google Privacy Policy, *supra* note 98.

128. *See* CAL. HEALTH CARE FOUND., NATIONAL CONSUMER HEALTH PRIVACY SURVEY 2005: EXECUTIVE SUMMARY 4 (2005), http://www.chcf.org/documents/healthit/ConsumerPrivacy2005ExecSum.pdf ("66 percent of respondents felt their paper medical records are 'very secure' or 'somewhat secure,' contrasted with 58 percent of those who felt their records are more secure in an electronic format.").

129. *See supra* Part III.A.

130. *See supra* Part II.A.

131. Though not within the scope of this Note, this assertion raises another question: should a new PHR regulatory scheme be only domestic, or is it an international issue? Theoretically, PHRs would be used globally, and thus may be subject to various international privacy laws. Another issue that may arise in this international privacy law debate is where the data is stored. Google recently patented a plan for a "water-based data center," a barge filled with servers and powered by ocean waves. *See* Ashlee Vance, *Google's Search Goes out to Sea*, N.Y. TIMES, Sept. 7, 2008, http://bits.blogs.nytimes.com/2008/09/7/googles-search-goes-out-to-sea.

even before HIPAA was enacted.[132] The privacy and security safeguards of HIPAA should not end at the doors of a health care facility but should extend to PHR vendors, who store the same sensitive health information as covered entities.

Finally, because patient PHI stored in a PHR is "in the cloud," it may be more vulnerable to unauthorized access than data stored electronically within a health care facility. Computer hackers routinely gain access to others' email and other online accounts, waging a constant war against computer programmers who attempt to secure user data.[133] PHRs should be required to employ best practices in data encryption, password protection, and authentication in order to safeguard PHI stored on their servers. Although many PHR vendors offer their services for free, they should not be held to a lower standard in regard to data quality and integrity. If they choose to offer PHR services, then vendors must comply with industry-best data security practices, given the nature of the data. Such practices should be determined by the HHS Secretary in conjunction with technical advisement from experts in computer technology.

Some may argue that Google and other PHR vendors are actually better equipped to secure health care information, as their sole business is information technology.[134] Although this may be true, it is important to establish national standards so newcomers to the industry have a cognizable framework for data security. The information contained in PHRs is too sensitive to simply rely on PHR vendors establishing their own privacy standards.

---

132. *See* Doe v. Se. Pa. Transp. Auth., 72 F.3d 1133, 1138 (3d Cir. 1995) ("An individual using prescription drugs has a right to expect that such information will customarily remain private."); United States v. Sutherland, 143 F. Supp. 2d 609, 611 (W.D. Va. 2001) ("[F]ederal courts have acknowledged the importance of protecting patient privacy in medical records.").

133. *See, e.g.*, Kim Zetter, *Alleged Palin E-Mail Hacker: It Was Easy*, ABCNEWS.COM, Sept. 18, 2008, http://abcnews.go.com/Technology/story?id=5835422&page=1.

134. Posting of NerveGas to Slashdot, http://science.slashdot.org/article.pl?sid=08/02/22/0020211&from=rss (Feb. 22, 2008, 00:08 EST) ("Google has a much better idea of how to warehouse data, manage access to it, and audit usage and access than any of the individual health care companies out there. They may not be perfect, but they'll probably do a whole lot better than what we/you have now.").

CONCLUSION

PHRs offer many benefits to patients. A patient's PHR is accessible from all over the globe and allows the patient's health care provider to make informed decisions on care and treatment in consultation with the patient's full medical history. Such a tool would have saved John's life, but without a PHR, his doctors had to rely on their best judgment and what they knew about their patient at the time—which was close to nothing. Patients managing chronic illnesses or conditions will be empowered through the use of PHRs and will likely reap the benefits of closer monitoring and understanding of their conditions.

Although the benefits offered by PHRs are substantial, the problem of privacy may stand in the way of widespread PHR adoption. Consumers worry about the privacy of their personal data, especially their health care information. There is currently a gap in health care privacy law—there are no direct regulations or rules for how PHR data is stored, accessed, or disclosed. The information in a PHR is the same information that is in a medical record held by a covered entity under HIPAA and should be afforded the same or even greater privacy protection. The safeguards of HIPAA are a good starting point, but in promulgating new rules to govern PHRs, the HHS Secretary should take into account the public policy behind widespread PHR adoption, the barrier that the lack of privacy imposes, the nature of the data contained in PHRs, and the unique "cloud computing" aspect that necessitates technical safeguards.

Colin P. McCarthy[*]

* J.D. Candidate 2010, William & Mary School of Law; B.A. 2007, Christopher Newport University. Thanks to my family and friends, especially my parents, Pat and Dianne, for their constant love and support.