Redefining “User-friendliness”: Privacy Concerns Related to Non-HIPAA Covered Internet Personal Health Records

By Kelly Walla, J.D., LL.M. candidate

Few can argue with the assertion that the information superhighway has revolutionized the world’s access to data over the last twenty years. For even the most technologically-challenged person, basic internet service ensures that a wealth of information is—quite literally—available at one’s fingertips. The convenience and “user-friendliness” that are the sine qua non of the internet are no small feats of technology. With the internet’s ease of operation and accessibility to the average person, the benefits of the internet are considerable and far-reaching. Internet access is now deemed vital to individuals functioning in personal, academic and professional contexts. This progress, however, has come with a significant cost to one of the values traditionally held sacrosanct by the American public, namely privacy. In the age of the internet, privacy is now an elusive and—in some circumstances—unattainable concept. Once information is posted to and accessed through the internet, the proverbial genie is potentially out of the bottle and will be difficult, if not impossible, to contain again.

An Introduction to Internet-Based Personal Health Records

Concerns about the internet’s affect on privacy are long-standing and have generally focused on the privacy and security of basic personal or financial information, such as that implicated in identity theft crimes. The recent emergence of internet-based personal health record (PHR) systems, however, has brought internet privacy to the forefront in a new context—that of health information.

Although many definitions of a PHR exist, it appears that many are moving towards defining a PHR as “a health record about a consumer that includes data gathered from different sources (e.g., health care providers, insurers, the consumer and third parties such as gyms and others) and is made accessible, often online, to the consumer and to those authorized by the consumer.”1 PHR programs come in many different forms, but this article focuses on internet-based programs.

The fundamental goal of internet PHR programs is to promote consumer empowerment and quality improvement in health care by facilitating the patient’s access to his personal health records and by serving as a centralized database for health information. PHRs are designed to enhance continuity of care by remedying the perceived problem of medical records being scattered among different health care providers. Additionally, many PHRs also offer the promise of increasing efficiency in health care delivery by enabling patients to communicate with providers and to access treatment plans remotely, as well as by

---

providing a more comprehensive record of the patient’s treatment so that duplicative tests are less likely to be ordered by different physicians.²

The features of each PHR program differ, but many contain the following features: (1) medical history information, (2) prescription list and refill information, (3) test results, (4) drug alerts, (5) immunization tracking, and (6) updated care plans.³ PHRs may also include other health-oriented capabilities that have not traditionally been associated with one’s medical record, such as email functions, “informational websites, niche search engines, articles, surveys, software downloads, and a host of other offerings …”⁴

PHR vendors include such diverse individuals and corporations as insurers, technology companies, and health care providers.⁵ In the last few months, many large corporations have announced plans for future PHR programs or PHR pilot projects. Among the big name tech companies that have recently thrown their hats into the PHR ring are Microsoft and Google.⁶

**Internet-Based PHRs and HIPAA**

In the wake of a flurry of publicity surrounding internet-based PHRs in general, the World Privacy Forum (WPF), a nonprofit public interest research group focused on privacy matters, issued two statements detailing privacy concerns related to PHRs.⁷

Without naming any specific programs, the WPF’s reports focus primarily on the issues that may arise for internet-based PHR programs that are not covered by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA is a federal law with implementing rules that provide certain minimum protections for “protected health information” held by “covered entities,” which generally include health plans, clearinghouses, and health care providers (e.g., physicians and hospitals) who utilize electronic means of handling health information in connection with certain transactions.⁸ The WPF states that in their current form, many PHRs will not be covered by HIPAA because the vendors do not fall within the definition of a “covered entity.” Instead, some of these vendors are commercial entities, which may operate outside the direct authority of HIPAA.⁹

---

³ *Id.*
⁴ Gellman, *supra* note 1 at 4.
⁵ *Id.* at 3.
⁸ See generally, 45 CFR Part 160 and Part 164, Subparts A and E.
⁹ Gellman, *supra* note 1 at 3-4.
Some commentators, however, have speculated that it might be possible for certain individual commercial PHRs to be bound by HIPAA standards if they were to execute business associate agreements with a covered entity. Under HIPAA, “business associates” are generally individuals or entities that perform functions for or on behalf of covered entities that require the transmission of individually identifiable health information. Among a business associate’s functions are such activities as legal, management, administrative, data aggregation, and financial functions. Covered entities must have agreements with business associates holding them to standards of use and disclosures consistent with HIPAA. Robert Gellman, an attorney and policy consultant with WPF, however, asserts that if a patient consents to the transfer of protected health information, a business associate agreement may not be necessary even under those circumstances.

Notably, the news media have reported that neither Google nor Microsoft has entered into a business associate agreement under HIPAA for their pilot programs. Both companies have stated a general commitment to the privacy of personal health information and have stated that the reason for their current lack of HIPAA business associate agreements is the developmental status of their programs. Gellman, however, expressed skepticism that Google or Microsoft would ever enter into business associate agreements with participating clinics, because such an agreement would impede efforts at marketing data.

PHRs may also voluntarily adopt protections similar to HIPAA through their privacy policies, but this will vary depending on each program. Google has declined to release its privacy agreement, due to the pilot status of its program. Thus, the precise nature of its privacy protections, and the protections afforded by many other PHR programs in development, are unknown at this time.

The World Privacy Forum’s Concerns Related to Non-HIPAA Covered PHRs

---

10 See generally, Joseph Conn, Microsoft, Mayo PHR lacks HIPAA Protection, MODERN HEALTHCARE ONLINE, Feb. 25, 2008 (implying that a business associate agreement might be fitting for certain commercial PHRs by inquiring as to the presence of HIPAA business associate agreements related to the development program between the Mayo Clinic and Microsoft, as well as the pilot program between Google and the Cleveland Clinic).
11 U.S. Dep’t. Health and Human Services, Office for Civil Rights, Summary of the HIPAA Privacy Rule, available at http://www.hhs.gov/ocr/privacysummary.pdf [hereinafter “OCR Privacy Rule Summary”]. Note that if a PHR vendor is performing the record maintenance function on behalf of the individual and not the covered entity, it is unclear whether it would fall within the definition of a “business associate.”
12 See Gellman, supra note 1 at 16.
13 Conn, supra note 10.
14 Id.; see also Joseph Conn, Google PHR Pilot has Caveat: No HIPAA Protection, Modern Healthcare Online, Feb. 22, 2008 [hereinafter Google PHR Pilot].
15 Conn, supra note 10 (stating that Mayo did not have a business associate agreement in place with Microsoft because it was still in the “concept and vision and strategy” phase.” Additionally, stating that the Cleveland Clinic did not have a business associate agreement with Google, because it is in its pilot stage).
16 Id.
17 Google PHR Pilot, supra note 14.
The WPF points out that without HIPAA protections, consumers are generally left to those privacy protections afforded under the PHR’s privacy policy, which may be subject to change without notice. Thus, although most internet-based PHRs state that the patients control disclosures of the information, there is a potential for consumer confusion. It is, therefore, imperative that consumers educate themselves as to the program-specific requirements of any non-HIPAA covered PHR they consider using in order to prevent leakage of information to marketers, employers, insurance companies, drug companies or any other unintended person.

Additionally, the WPF states that consumers should be aware that the use of some non-HIPAA covered PHRs may potentially impact the patient’s rights regarding issues such as physician-patient privilege, subpoenas, and marketing of information. First, the WPF points out that use of non-HIPAA covered PHRs may potentially limit the availability of the physician-patient privilege to patients involved in litigation. The physician-patient privilege is a state-specific law that enables the patient to prevent the physician from being compelled to disclose certain confidential communications in litigation. The physician-patient privilege is not absolute and is subject to many exceptions, which vary depending on the applicable law. One of the biggest, and most common, exceptions is waiver of the privilege by disclosure to third parties. In many states, the communication must truly be confidential in order for the patient to avail himself of its protections. It is unclear whether a disclosure to a PHR would be deemed a waiver of the privilege. This may, however, be one avenue for attorneys to attack the physician-patient privilege, potentially to the patient’s detriment.

Second, under HIPAA, patients are generally entitled to notice of subpoenas issued upon covered entities seeking production of the patients’ medical records. This notice is important, because it provides the patient with an opportunity to limit or challenge the subpoena through objections or by seeking a protective order. The WPF points out that if such notice is not provided for under a privacy policy for a non-HIPAA covered PHR, patients may not have notice of the subpoena and, therefore, may lose this important procedural safeguard.

Finally, HIPAA contains basic protections from disclosing health information for marketing purposes. Non-HIPAA-covered PHRs would generally not be subject to these limitations. Thus, there may be a greater potential for the marketing of patient’s health information unless the vendor agrees otherwise or a state law provides protection against marketing. The WPF contends that “even if a PHR vendor states that it does not share information with marketers without consent, it may … still be easy for the vendor

---

18 Note that there may be state law protections in addition to federal HIPAA law and regulations.
19 Gellman, supra note 1 at 15.
20 See, e.g., Kornblum, supra note 6.
21 Gellman, supra note 1 at 5-6.
22 45 C.F.R. § 164.512(e).
23 Gellman, supra note 1 at 6-7.
24 Id.
25 See generally, 45 C.F.R. §§ 164.501 and 164.508(a)(3); see also Gellman, supra note 1.
26 See Gellman, supra note 1 at 7.
to induce consumers to give consent without actually realizing what they are doing.”

This may occur through such methods, as patients blithely checking a consent box without reading all the information contained in the consent form.

Conclusion

The gathering of health information for access through the internet generates new privacy concerns when the PHRs are not covered by HIPAA. Few things are as sensitive and personal as health information. Health care providers are entrusted with the most intimate and sometimes embarrassing or stigmatizing details of their patients’ lives. This is the very reason that the state and federal statutory and common law has made physician-patient confidentiality/privilege and privacy an integral part of the body of general health law.

Although the goals of internet-based PHRs are praiseworthy in promoting efficiency and consumer participation in healthcare decisions, the privacy implications must also be considered by patients prior to agreeing to participate in such programs. Determining whether an individual program is “user friendly” may necessitate a weighing of the individual consumer’s desire for convenience with his comfort level with the privacy protections afforded under a particular PHR program. PHRs generally state that they have a commitment to privacy, but there may be wide variations in the protections afforded by different PHRs. If an individual PHR program is not covered by HIPAA, then certain basic protections may not be present. In instances of non-HIPAA covered internet PHRs, transparency of privacy protections is key. Patients must act as rational consumers and thoroughly review the specific requirements of a program and, as WPF states, “read the fine print” of the privacy policy of each individual PHR program. Otherwise, the consumer may get more (or less in terms of privacy) than that for which he believed he was bargaining.


---

27 Id.
28 Id. at 8; see also Gellman and Dixon, supra note 7 at 3-4.
29 Gellman and Dixon, supra note 7 at 4.