PRIVACY AND SECURITY OF PERSONAL HEALTH RECORDS MAINTAINED BY ONLINE HEALTH SERVICES

Jenna Caldarella

TABLE OF CONTENTS

I. INTRODUCTION

Online health services, such as Google Health and HealthVault, offer the option of maintaining a personal health record ("PHR") on the Internet.[1] These services are not covered entities under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and they are not subject to the Act's Privacy Rules.[2] The Federal Government needs to enact legislation that would hold these online health services to the same standards of privacy as those entities covered under HIPAA.

A PHR is a way for people to store, collect, and share important health information.[3] PHRs "serve to lower prices, ease paperwork and give consumers control over their medical histories."[4] Many websites offer ways for people to store PHRs electronically. Consumers can gather health information from various institutions, such as pharmacies, hospitals, and health insurance companies, and store this information on these websites.[5]

While PHRs offer consumers this benefit, there are also negative consequences to having PHRs available electronically. Consumers will face potential privacy issues when storing PHRs electronically.[6] Most of the sites on which individuals can store PHRs are not covered entities under HIPAA; therefore, the HIPAA privacy standards do not apply to these sites.[7] Consequently, these sites do not have to comply with the

[1] John D. Halamka, *Your Medical Information in the Digital Age*, HARV. BUS. REV., July 2009, *available at* http://hbr.harvardbusiness.org/web/2009/health/your-medical-information-in-digital-age?cm_mmc=npv-_-TOPICEMAIL-_-JUL_2009-_-TECH.

[2] myPHR, *Your Privacy Rights*, http://www.myphr.com/index.php/privacy_and_phrs/your_privacy_rights/ (last visited Dec. 20, 2009).

[3] myPHR, *What is a PHR?*, http://www.myphr.com/index.php/start_a_phr/what_is_a_phr/ (last visited Dec. 20, 2009).

[4] Patricia Lopez, *Pawlenty Unveils Plan to Revamp Healthcare System in Minnesota*, STAR TRIB.(Minn.-St.Paul, Minn.), Jul. 29, 2008, *available at* http://www.startribune.com/politics/state/26082889.html?location_refer=$urlTrackSectionName.

[5] *See, e.g.,* Google Health, Frequently Asked Questions, http://www.google.com/intl/en-US/health/faq.html#phr (last visited Dec. 20, 2009) (stating that a user may import medical records from hospitals and neighborhood pharmacies).

[6] ROBERT GELLMAN, THE WORLD PRIVACY FORUM, PERSONAL HEALTH RECORDS: WHY MANY PHRS THREATEN PRIVACY 2–8 (2008), *available at* http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf.

[7] *See, e.g.,* Google Health, Privacy, http://www.google.com/intl/en-US/health/about/privacy.html (last visited Dec. 20, 2009).

minimum standards of security that covered entities do. Many consumers are unaware of this fact.[8]

Recently, hospitals, which are covered entities under HIPAA, have been experiencing privacy issues regarding patients' health records. In 2008, approximately 127 employees at the UCLA Medical Center were caught improperly viewing health records of celebrities.[9] There are possibly countless other instances of health record spying that have gone unreported. As a result, California legislators passed a bill requiring hospitals to implement stronger security measures to safeguard patient information and hold individuals accountable for violating patient information safety measures.[10]

According to the Federal Trade Commission, approximately 250,000 people were victims of medical identity theft in 2005.[11] This number accounted for only three percent of the 8.3 million victims of reported identity theft.[12] The cost of medical identity theft in the United States alone is approximately $1 billion.[13] "The consequences of [identify thefts]. . . include annoyance and distraction, financial loss, direct violation of federal and state law resulting in penalties, and of course, long-term institutional damage to an organization's [or person's] reputation."[14] Congress found that the American public has become more concerned with

---

[8] GELLMAN, *supra* note 6, at 4–5.

[9] Charles Ornstein, *More UCLA Medical Center Employees Peeked at Celebrities' Records, State Says*, L.A. TIMES, Aug. 5, 2008, *available at* http://articles.latimes.com/2008/aug/05/local/me-health5; *Cf.* Alexandra Zavis, *Former Cedars-Sinai Employee Held in Identity Theft, Fraud*, L.A. TIMES, Dec. 23, 2008, *available at* http://articles.latimes.com/2008/dec/23/local/me-cedars-sinai23 (describing how a hospital worker was charged with identity theft and fraud after "us[ing] the names of actual workers' compensation beneficiaries to submit claims for services that were never performed" at a fictitious lab created by the perpetrator).

[10] Patrick McGreevy, *New Oversight, Stiffer Penalties Approved for Snooping into Patient Records*, L.A. TIMES, Aug. 27, 2008, *available at* http://articles.latimes.com/2008/aug/27/local/me-legis27.

[11] Beth Wilson, *Medical Identity Theft is Often an "Inside Job"*, AM. MED. NEWS, Mar. 3, 2008, *available at* http://www.ama-assn.org/amednews/2008/03/03/prsc0303.htm.

[12] Privacy Digest, *New FTC Statistics Affirm World Privacy Forum's 2006 Medical Identity Theft Report*, http://www.privacydigest.com/2007/11/29/new+ftc+statistics+affirm+world+privacy+forums+2006+medical+identity+theft+report. (Nov. 29, 2007, 19:00 EST).

[13] Kurt Long, *The Grave Costs of Medical Identity Theft*, ADVANCE FOR HEALTH INFO. PROFLS., Oct. 6, 2006, http://health-information.advanceweb.com/Article/The-Grave-Costs-of-Medical-Identity-Theft-2.aspx.

[14] *Id.*

the privacy and security of personal health information ("PHI") because of the increased number of breaches of personal information and the "numerous reports of the inadequacy of the security of electronic networks."[15] With the recent push by the Federal Government for healthcare providers to convert patient records to an electronic health record ("EHR"), and the introduction of services that would keep PHRs on the internet, the possibility of an increase in both the cost and number of victims of medical identity theft looms large.

The first section of this paper will discuss the recent development of online health services and their purpose. The second section will give a brief overview of the HIPAA Privacy Rule, and it will explain why online health services fall outside of the scope of the Privacy Rule. Because online health services are not covered by HIPAA, this section will also discuss how these sites enforce their privacy policies and address whether members can sue for breach of confidentiality or fiduciary duty. The third section will discuss bills at both the federal and state level that address entities with access to individually identifiable health information that are not covered by HIPAA. Finally, this paper will conclude with recommendations for proposed legislation to address the emergence of online health services.

II. ONLINE HEALTH SERVICES

A. Services Provided by Online Health Services

In 2007, Microsoft launched one of the first online health services where individuals can manage and store PHRs.[16] This service is called HealthVault. In 2008, Google launched its own online health service called Google Health.[17] The popular medical website WebMD also offers the public an easy way to store PHRs.[18] These are some examples of online health services

[15] Technologies for Restoring Users' Security and Trust in Health Information Act of 2008, H.R. 5442, 110th Cong. § 2(a)(4) (2d Sess. 2008).

[16] Posting of Jacob Goldstein to Wall St. J. Health Blog, http://blogs.wsj.com/health/2007/10/04/microsoft-beats-google-on-health-launch (Oct. 4, 2007, 10:17 EST).

[17] Christopher Lawton & Ben Worthen, *Google to Offer Health Records on the Web*, WALL ST. J., Feb. 28, 2008, *available at* http://online.wsj.com/article/SB120416090319398335.html.

[18] *See* WebMD, Personal Health Record, http://www.webmd.com/phr (last visited Dec. 20, 2009) (requiring new users to follow simple steps to register on the website before uploading their information).

that allow individuals to store, organize, and manage individually identifiable health information on the internet through their websites.[19] Online health services have partnered with pharmacies, hospitals, clinics, and other healthcare institutions to help consumers gather information for PHRs.[20] These sites claim that storing PHRs electronically is an easy way to manage personal health information, share that information with authorized care providers, and maximize health benefits.[21]

Companies that have been part of the health industry for years have begun to provide these services as well. Insurance companies, such as UnitedHealth Group, have launched websites for individuals to store PHRs.[22] Other insurance companies, for instance, Aetna and WellPoint, allow their health plan members to view their digital-health records on the companies' websites.[23] Some of these insurance companies, Aetna for example, are teaming up with online health services "to help patients access all of their health info in one place and transfer it easily to doctors or hospitals, among others."[24] In addition, Blue Cross Blue Shield of Massachusetts teamed with Google Health in 2008 to allow its members to send claims information to Google

[19] *See* Google Health, http://www.google.com/health (last visited Dec. 20, 2009) (enabling users to organize health information, gather medical records, and share information with family, doctors or caregivers); *see also* Microsoft HealthVault, http://www.healthvault.com/Personal/index.html (last visited Dec. 20, 2009) (enabling users to organize health information in one location by entering it once, and gain insight with information to make informed decisions); WebMD, Personal Health Record, http://www.webmd.com/phr (last visited Dec. 20, 2009) (enabling users to gather, store and manage health information, share information with care providers).

[20] *See, e.g.,* Steve Lohr, *Google Offers Personal Health Records on the Web*, N.Y. TIMES, May 20, 2008, *available at* http://www.nytimes.com/2008/05/20/technology/20google.html?_r=2&oref=slogin (providing examples of a Cleveland, OH doctor whose clinic's records are linked to the Google record and citing companies such as Walgreens and CVS who are partners with Google Health); Posting of Sarah Rubenstein to Wall St. J. Health Blog, http://blogs.wsj.com/health/2008/10/22/aetna-links-up-with-microsofts-healthvault/ (Oct. 22, 2008) (citing Aetna and Blue Cross Blue Shield of Massachusetts as insurers who will allow members to use Google Health).

[21] *See* Lohr, *supra* note 20 (asserting that the use of PHRs will aid in maintaining treatment communication between a patient's different physicians).

[22] Victoria Knight, *UnitedHealth Takes on Microsoft, Google with Online Health Venture*, Wall St. J. Health Blog, http://blogs.wsj.com/health/2008/12/01/unitedhealth-takes-on-microsoft-google-with-online-health-venture/ (Dec. 1, 2008, 17:12 EST).

[23] *Id.*

[24] Rubenstein, *supra* note 20.

Health.[25] Unlike HealthVault and Google Health, however, these insurance companies are covered entities under HIPAA and therefore are subject to the HIPAA Privacy Rule.

B. Protections Offered by Online Health Services

Google Health specifically states on its Privacy webpage that it is not covered by HIPAA and is not subject to the HIPAA Privacy Rule.[26] Although HIPAA does not apply to Google Health, the service's privacy policy is very similar to the HIPAA Privacy Rule.[27] Google Health promises its users that it will not sell, rent, or share information with others unless the user specifically authorizes the dissemination of information.[28] Instead, the users are responsible for gathering and maintaining the records and sharing it with individuals and entities of their choosing.[29] However, Google provides the user with limited situations where it will share information with others, without users' consent, including situations in which Google is required by law to reveal the medical information.[30] In addition, Google can use the information users store on its site to publish aggregate trends and statistics.[31] But these statistics are not linked to the individuals and are only used for analytical purposes.[32]

Microsoft provides in its HealthVault privacy statement that it will not share PHRs without the consent of the user. [33] Like

[25] *Id.*

[26] Google Health, *Google Health Puts You in Control of Your Health Records*, http://www.google.com/intl/en-US/health/about/privacy.html (last visited Dec. 20, 2009).

[27] Google Health, *Google Health and HIPAA*, http://www.google.com/intl/en_us/health/hipaa.html (last visited Dec. 20, 2009) (comparing the HIPAA Privacy Rule to Google Health's privacy policy in a chart); *see also infra* Part II.

[28] Google Health, *Google Health Privacy Policy*, http://www.google.com/intl/en-US/health/privacy.html (last visited Dec. 20, 2009).

[29] *See id*.

[30] Google Privacy Center, http://www.google.com/intl/en/privacypolicy.html (last visited Dec. 20, 2009) (listing other situations where Google will share personal information, including complying with the Google Terms of Service or any violations of the terms; detecting, preventing, or addressing fraud and security issues; or to "protect against [imminent] harm to the rights, property or safety of Google, its users or the public as required or permitted by law.").

[31] *Id.*

[32] *See id.* (sharing aggregated, non-personal information with third parties does not identify individual users).

[33] HealthVault, HealthVault Account Privacy Statement, https://account.healthvault.com/help.aspx?topicid=PrivacyPolicy (last visited Dec. 20, 2009) [hereinafter *Health Vault*].

Google Health, HealthVault also reserves the right to share information without a user's authorization in limited circumstances.[34] In addition, HealthVault uses the personal information to provide information about HealthVault to the user.[35]

Also similar to Google Health, HealthVault allows users to control who sees their information.[36] HealthVault provides its users with various options for sharing PHRs.[37] Users can grant other individuals or entities the ability to view and/or modify one's PHRs.[38] For example, a user may allow a family member or healthcare provider "view-only access" or "view-and-modify access," both time-limited access programs.[39] Additionally, a user may grant another person custodial access. Custodial access is usually reserved for a spouse or family member of the user.[40] Under this access program, the custodian may read, change, or delete the PHRs, and revoke or grant others any type of access to the records, including custodial access.[41]

HealthVault states on its Privacy webpage that it complies with the HONcode standard for trustworthy health information, which requires online companies in compliance with this code to "[r]espect the privacy and confidentiality of personal data submitted to the site by the visitor."[42] HONcode is an ethical code for websites that electronically store medical and health information.[43] In addition, HealthVault, in compliance with HONcode, promises to "undertake to honour or exceed the legal

[34] *See id.* (sharing information without authorization by HealthVault will only occur in three instances: to comply with the law, when protecting or defending Microsoft property, and to protect the personal safety, welfare, and privacy of Microsoft users or services.)

[35] *Id.*

[36] *Id.*

[37] *See id.* (listing the levels of access that can be granted to individuals other than the custodian of the PHR).

[38] *Id.* (enabling the consumer, as a custodian of his/her account, to grant levels of access to other Service users, which allow other users to help the consumer update and manage the EHR).

[39] Microsoft HealthVault Account Privacy Statement, *supra* note 33.

[40] *Id.*

[41] *Id.*

[42] Health on the Net Foundation, The HONcode in Brief, http://www.hon.ch/HONcode/Conduct.html (last visited Dec. 20, 2009) [hereinafter *HONcode in Brief*].

[43] Health on the Net Foundation, Quality & Trustworthiness of the Medical & Health Web, http://www.hon.ch/HONcode/Visitor/visitor.html (last visited Dec. 20, 2009).

requirements of medical/health information privacy that apply in the country and state where the Web site and mirror sites are located."[44] However, HealthVault warns its users that the privacy policy may be updated or changed at any time.[45] While HealthVault promises to alert users to important changes in the privacy policy, some online health services may change their policy "without notice, and without the user's ability to object."[46]

C. Protections Not Provided by Online Health Services

NeitherGoogle Health nor HealthVault permit advertisements to fund their site.[47] However, other "PHR vendor[s]"[48] may permit advertising that can result in a user unwittingly offering access to his or her PHRs:

> [F]or example, . . .a PHR contains blood pressure readings for the last few years. An advertisement about blood pressure medicine appears when the consumer reads the PHR record, and it says *click here for an analysis of your actual blood pressure results*. The PHR accepts that click as authorization, and the effect is that the consumer has unwittingly and irretrievably disclosed his blood pressure and perhaps other personal information to the company that placed the ad. The advertiser who obtained the information with this "consent" may then save, use, and redisclose the information at will, depending on the privacy policy in effect. [49]

With such a digital consent, a user need only click on a link or check a box at the end of a lengthy, small-print disclosure policy. This can lead to more users unknowingly sharing their PHRs with companies or individuals with whom they never intended to share that information.

It is obviously in the best interest of these online health services to protect the PHI of its consumers. Otherwise, consumers will not trust online health services to keep PHI safe and will choose alternative options for storing health records electronically. However, without HIPAA regulation, it is up to each individual PHR vendor or online health service to determine

---

[44] HONcode in Brief, *supra* note 42 (follow "complete version" hyperlink under "3. Privacy").

[45] HealthVault, *supra* note 33.

[46] GELLMAN, *supra* note 6, at 15.

[47] Google Health, http://www.google.com/intl/en-US/health/faq.html#free (last visited Dec. 20, 2009).

[48] GELLMAN, *supra* note 6, at 8.

[49] *Id.* at 13.

whether its consent policies are adequate.[50] HealthVault tells consumers in its privacy policy that it uses Secure Sockets Layer (SSL), which "encrypts the information to help prevent others from reading it while it's in transit from your computer to the HealthVault Service."[51] Even if the online health service uses state-of-the-art technology, there are no guarantees that the PHI will remain secure.[52]

In addition to online health services, the federal government is pushing for a nationwide system for maintaining EHRs. The economic stimulus package proposed in 2009 provides incentives for doctors to switch from paper records to EHRs.[53] Doctors using the EHRs in a "'meaningful'" way would receive reimbursements from Medicare.[54] However, this bill is meeting resistance for several reasons. First, some are concerned that the bill, which includes $20 billion for "health-care information technology," is excessive, especially since the bill is funding technology that is not even in existence yet.[55] Second, many doctors are wary of switching over from paper records to EHRs.[56]

Doctors are not the only people who remain unconvinced that EHRs are a viable solution to healthcare issues. Patients are also concerned with privacy issues and having correct information in their records.[57] While the federal government's

---

[50] *See id.* at 13–14.

[51] HealthVault, *supra* note 33.

[52] GELLMAN, *supra* note 6, at 12 ("[T]he uncertainty about the security, about the transmission of data between a person's computer and the PHR, or about the security of any information downloaded from the PHR to a personal computer remains. Nothing will ever eliminate security concerns when a third party is holding data.").

[53] Doug Trapp, *Medicaid, Health IT to See Billions From Stimulus Package Signed by Obama*, AM. MED. NEWS, Feb. 23, 2009, *available at* http://www.ama-assn.org/amednews/2009/02/23/gvl20223.htm.

[54] Jacob Goldstein & Jane Zhang, *Waste Feared in Digitizing Patient Records*, WALL ST. J., Jan. 22, 2009, *available at* http://online.wsj.com/article/SB123258818514104775.html (including "coordinating a patient's care with other providers and reporting clinical quality measures.").

[55] *Id.*

[56] *Id.*

> A study published last year in the New England Journal of Medicine found that only 4% of U.S. physicians were using "fully functional" electronic health-records systems. What's more, simply installing new IT systems in doctors' offices isn't enough. The systems have to be able to talk to each other, so doctors and hospitals can share information. And doctors and nurses have to learn how to use the systems in ways that help patients.

Id.

[57] *See id.*

goal is to have widespread use of EHRs by 2014, some argue that the current stimulus bill is too hasty because the bill is fast-tracking the health-care information technology system, which could lead to inadequate training and installation of the system,[58] and not focusing on safeguarding the information in the EHRs. This could create a bad experience for both doctors and patients.

III. PROTECTIONS HIPAA PROVIDES

HIPAA is a federal regulation which provides methods for maintaining the safety and security of "individually identifiable health information."[59] HIPAA aims to "improve portability and continuity of health insurance coverage in the group and individual markets, . . . [and] to simplify the administration of health [care.]"[60] Subpart E of Part 164 of the regulations promulgated under the authority of HIPAA governs the "[p]rivacy of [i]ndividually [i]dentifiable [h]ealth [i]nformation."[61] This is known as the HIPAA Privacy Rule.

The Privacy Rule protects "[p]rotected health information," or PHI, that is "[t]ransmitted by electronic media; [m]aintained in electronic media; or [t]ransmitted or maintained in any other form or medium[,]" including paper or oral transmissions, by a covered entity.[62] PHI includes:

> [D]emographic information collected from an individual, and: [i]s created or received by a [covered entity]; and [r]elates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual; and [t]hat identifies the individual; or [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.[63]

There are three types of HIPAA-covered entities: "[a] health

---

[58] *Id.*

[59] Brief for the Respondents in Opposition at I,S.C. Med. Ass'N v. Thompson, 540 U.S. 981 (2003) (No. 03-114), *available at* http://www.usdoj.gov/osg/briefs/2003/0responses/2003-0114.resp.pdf; US Department of Health & Human Services, Health Information Privacy, http://www.hhs.gov/ocr/privacy/ (last visited Dec. 20, 2009).

[60] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (to be codified at 42 U.S.C. § 201).

[61] Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.500 (2008).

[62] 45 C.F.R. § 160.103 (2008).

[63] *Id*.

plan[, a] healthcare clearinghouse[, and a] healthcare provider."[64] To be a HIPAA covered entity, the provider must electronically transmit health information.[65] This requirement seems to exclude online health services as providers because these services do not electronically transmit health information. They merely allow third parties to access the PHI on the website.[66] Based on the HIPAA definitions of each of these covered entities, online health services do not fit into any of the three categories.[67]

Health plans are plans, for either individuals or groups, that pay for the individual's or the group's medical care.[68] Examples of health plans covered by HIPAA include "health, dental, vision, and prescription drug insurers, health maintenance organizations ('HMO'), Medicare, [and] Medicaid."[69] Online health services are not health plans because they are not plans that provide or pay the cost of medical care. In fact, the online health services are not plans at all; rather, they are storage facilities of PHI.

The second type of covered entity is a healthcare clearinghouse. A healthcare clearinghouse is an entity that either "[p]rocesses. . . health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction[,]" or "[r]eceives a standard transaction from another entity and processes. . . health information into nonstandard format or nonstandard data content for the receiving entity."[70] Healthcare clearinghouses usually receive individually identifiable health information when they provide services to covered health plans or healthcare providers.[71] Online health services are not healthcare clearinghouses because they do not process

64 *Id.*

65 *Id.*

66 *See* Google Health, *Google Health Privacy*, http://www.google.com/intl/en-US/health/about/privacy.html (last visited Dec. 20, 2009); Google Health, Privacy, and HIPAA, http://googlepublicpolicy.blogspot.com/2008/05/google-health-privacy-and-hipaa.html (May 19, 2008); Microsoft HealthVault and HIPAA, http://msdn.microsoft.com/en-us/healthvault/cc507320(printer).aspx (last visited Dec. 20, 2009).

67 *See* § 160.103.

68 *Id.*

69 U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE (2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf [hereinafter *Summary of HIPAA Privacy Rule*].

70 § 160.103.

71 Summary of HIPAA Privacy Rule, *supra* note 69, at 3.

information received from another entity. Instead, the online health service stores PHI that its customers upload to its site. An online health service only has contact with entities regarding PHI when an individual authorizes the online health service to send that specific information to the entity and when a hospital, pharmacy, or health insurance agency sends copies of PHI to the online health service for storage.

Healthcare providers include those entities that provide medical or health services and that transmit financial transactions for the healthcare of the patient.[72] When a healthcare provider "electronically transmits health information in connection with. . . transactions," such as "claims, benefit eligibility inquiries, [or] referral authorization requests," it is considered a covered entity.[73] The electronic transmission must be in connection with the health information of the patient.[74] Even when the healthcare provider "uses a billing service or other third party" to electronically transmit the health information, it becomes a covered entity.[75] Examples of healthcare providers include "all 'providers of services'. . . and 'providers of medical or health services'. . . as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for healthcare."[76] An online health service is not a healthcare provider because it does not provide for the healthcare of the individual using the service and is not involved in any electronic transactions of the individual.

Although the online health services do not fall into any of the categories of covered entities listed in the Privacy Rule, some of the six specific situations in which a HIPAA covered entity may use and disclose protected information are similar to situations where online health services may disclose PHI. First, a HIPAA covered entity may disclose PHI to the individual who is the subject of that information.[77] The purpose of online health services, which is to allow the subjects of PHI to access their own records, is identical to this permitted use or disclosure.[78]

Second, a HIPAA covered entity may use or disclose PHI where

[72] § 160.103.
[73] Summary of HIPAA Privacy Rule, *supra* note 69, at 2.
[74] § 160.103.
[75] Summary of HIPAA Privacy Rule , *supra* note 69, at 2.
[76] *Id.*
[77] § 164.502(a)(1)(i).
[78] Google Health, *About Google Health*, http://www.google.com/intl/en-US/health/about/index.html (last visited Dec. 20, 2009).

the individual is given the opportunity to agree to or reject to the use or disclosure of the information.[79] Online health services give individuals complete control over sharing the PHI with other entities (both those that are and are not covered by HIPAA) and individuals.[80] For example, a Google Health consumer must approve access to the PHI by any third-party website.[81]

Third, a HIPAA covered entity may use or disclose PHI for public interest and benefit activities.[82] Similarly, online health services will sometimes use the information in its consumers' PHI records in a general way in order to "aggregate data to publish trend statistics and associations" for its own statistical analysis; however, it is not necessarily for public interest or benefit.[83] If the use or disclosure does not fall within any of the abovementioned categories under HIPAA, the covered entity must receive written authorization by the individual.[84]

Further, online health services grant individuals similar rights pertaining to their PHI to those of the Privacy Rule. For example, HIPAA covered entities are required to provide notice of privacy practices to individuals.[85] An individual also has the right to review and access their PHI.[86] Individuals may also amend their PHI when the information is inaccurate or incomplete.[87] Online health services also grant individuals these

[79] § 164.510. The covered entity may orally inform and obtain an oral agreement from the individual regarding the use or disclosure of the PHI. *Id.* Additionally, where an individual is incapacitated or unavailable, or there is an emergency situation, the covered entity may use or disclose the individuals PHI without the individual's permission so long as the use or disclosure is determined to be in the individual's best interest. Summary of HIPAA Privacy Rule, *supra* note 69, at 6.

[80] Google Health, *Google Health Privacy Policy*, http://www.google.com/intl/en-US/health/privacy.html (last visited Dec. 20, 2009).

[81] *Id.*

[82] § 164.512. Examples of public interest and benefit activities include those required by law; public health activities; law enforcement purposes; reporting crime in emergencies; research purposes; and specialized government functions. *Id.*

[83] Google Health, *supra* note 80. The data used in the trend statistics and associations will not be personally identifying information. *Id.*

[84] Summary of HIPAA Privacy Rule, *supra* note 69, at 9*; see also* § 164.508 (listing uses and disclosures for which authorization is required).

[85] § 164.520(a)(1).

[86] § 164.524(a). This right does not apply to psychotherapy notes, information compiled for legal proceedings (both criminal and civil), laboratory results to which the Clinical Laboratory Improvement Act prohibits access, or PHI maintained by certain research laboratories. *Id.*

[87] § 164.526(a).

same three rights. First, online health services make their Privacy Statements readily available for customers on their website and encourage customers to review it periodically for updates. Second, the online health services grant the individual storing PHI the right to review and access the PHI and amend the record at any time.

An individual under HIPAA may also request an accounting of disclosures made in the previous six years.[88] The covered entity must comply with the individual's request in a timely manner, which is sixty days according to the Privacy Rule.[89] Many online health services also allow individuals to obtain a record of entities and individuals who have accessed the individual's PHI. However, these sites do not limit this record to any time frame. In addition, individuals can request that a HIPAA covered entity restrict the use or disclosure of PHI,[90] and request an alternative means or location for receiving PHI communications.[91]

Although online health services perform some similar services and grant similar protections to individuals regarding PHI that are offered under the HIPAA Privacy Rules, they do not fit into any of the definitions of the HIPAA covered entities. Therefore, HIPAA does not regulate online health services and individuals' whose privacy is breached by one of these services do not have a private course of action against the breaching service.

It is apparent that online health services are not regulated by HIPAA because the services do not function like HIPAA covered entities. Online health services allow individuals to store and manage the data on the website.[92] Healthcare entities may send an individual's PHI to the online health service for storage on the service website for the individual. However, when an online health service consumer directs a physician to send PHI to the

[88] § 164.528(a). There are several situations in which the Privacy Rule does not require a covered entity to account for a disclosure: to carry out treatment, payment and healthcare operations; to individual or personal representative of the individual of the PHI when excluded under § 164.502; incident to or otherwise permitted or required disclosures; pursuant to an authorization; for notification of or to persons involved in an individual's healthcare or payment for healthcare; for national security or intelligence purposes; to correctional institutions or law enforcement officials; or as part of a limited data set. *Id.*

[89] § 164.528(c). However, if the request is made for a disclosure before a covered entity's Privacy Rule compliance date, the covered entity is not required to account for such disclosure.

[90] § 164.522(a).

[91] § 164.522(b).

[92] *Id.*

service, the scope of HIPAA would not cover this disclosure. HIPAA treats this transaction as a disclosure to a third party, outside of the Privacy Rule protections. If the PHI is released to other third parties, the patient would not be able to sue the online health service or the doctor under HIPAA because "a court is likely to agree that the patient waived the [doctor-patient] privilege by consenting to the disclosure."[93]

Because these online health services are not covered entities under HIPAA, the Department of Health and Human Services (HHS) cannot impose civil or criminal penalties authorized by HIPAA for privacy breaches.[94] Instead, Google Health informs its customers that the Federal Trade Commission enforces privacy protections through civil and criminal penalties.[95] In addition, general consumer protection laws grant state attorneys general and district attorneys the authority to enforce Google Health privacy protections.[96]

IV. PROPOSED LEGISLATION REGARDING ONLINE HEALTH SERVICES

With the increase in awareness and use of online health services, legislation must be enacted to protect PHI that is stored on these websites. At the federal level, there are two bills of significance regarding PHI privacy:

A. Independent Health Record Trust Act of 2007

The first bill that could potentially regulate online health services is the Independent Health Record Trust Act of 2007.[97] One of the purposes of this bill is to "ensure[]. . .[the] privacy,

[93] GELLMAN, *supra* note 6, at 5.

[94] If a covered entity fails to comply with the requirements of the HIPAA Privacy Rule, the HHS may impose civil penalties of one hundred dollars per failure to comply. Pub. L. 104-191; 42 U.S.C. § 1320d-5 (2006). In addition, the Department of Justice can criminally sanction any person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA. Pub. L. 104-191; 42 U.S.C. §1320d-6 (imposing a fine of $50,000 and up to one-year imprisonment).

[95] Google.com, *Google Health and HIPAA*, http://www.google.com/intl/en_us/health/hipaa.html (last visited Dec. 20, 2009); *see also* 15 U.S.C.A. § 45(l) (West 2006) (indicating civil penalties for unfair methods of competition).

[96] *Google Health and HIPAA*, *supra* note 95.

[97] *See* Independent Health Record Trust Act of 2007, H.R. 2991, 110th Cong. (2007), as referred to the House Subcommittee on Health, July 17, 2007. No action on this bill has been taken since then.

security, and confidentiality" of PHI.[98] This bill encourages the use of EHRs of individuals in independent health record trusts (IHRT).[99] An IHRT is defined as "a legal arrangement under the administration of an IHRT operator that meets the requirements of this Act with respect to electronic health records of individuals participating in the trust or IHRT."[100] Participation in an IHRT program will be voluntary.[101] However, the bill offers doctors a financial incentive to convert patients' health records to EHRs.[102]

If an online health service fits the definition of an IHRT, then the service would have to act as an IHRT operator, having a fiduciary duty towards the participant, which requires the IHRT operator to act in the best interest, and for the benefit of the participant and the IHRT.[103] This is a duty that is not included under HIPAA, or any of the security regulations of online health services.[104] The bill also includes in the IHRT operator's

---

[98] *Id.* § 2(7).

[99] *See* H.R. 2991. This bill aims to:

> [I]mprove the availability of health information and the provision of healthcare by encouraging the creation, use, and maintenance of lifetime electronic health records of individuals in independent health record trusts and by providing a secure and privacy-protected framework in which such records are made available only by the affirmative consent of such individuals and are used to build a nationwide health information technology infrastructure.

Id.

[100] § 3(10).

[101] § 7(a).

[102] An IHRT may generate revenue by charging account fees for the trust, charging EHR data users for use of information in the trust, through the sale of the trust, and other activities deemed appropriate by the Federal Trade Commission. H.R. 2991 §8(a)-(d). However, healthcare providers are given incentives to access such records through the exclusion of fees for services specified by the IHRT. *Id.* § 8(b). Such services include the transfer of information provided by the healthcare provider to the EHR. *Id.* Furthermore, any revenue gained by a healthcare provider while using IHRT would not be included in that provider's gross income, this providing a tax break. *Id.* § 8(d). *See also* Marianne Kolbasuk McGee, *New Bill Proposes 'Health Record Trusts' that Pay Doctors to Use E-Health Records*, INFORMATIONWEEK, Jul. 26, 2007, *available at* http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=201201355 (explaining that doctors "could be financially rewarded for submitting authorized patient data to the trust through 'sharing' the trust's revenue").

[103] H.R. 2991 § 5(a)(1).

[104] *Compare* 42 U.S.C.A. § 1320d-2(d) (West 2003) (discussing the safeguards for the protection of electronic health information, imposing no duties beyond safeguarding the health information), *and* 45 C.F.R. §164.306 (2009) (setting out general security standards in order to protect electronic health records), *with* Google Health Privacy Policy, http://www.google.com/intl/en-US/health/privacy.html (last visited Dec. 20, 2009) (setting security measures and

fiduciary duties the duty to obtain the consent of the IHRT participant prior to releasing any information in the IHRT.[105] This is distinguishable from the HIPAA Privacy Rule where covered entities are required to obtain authorizations from an individual only if the disclosure is not one of the six permitted uses or disclosures for which a covered entity may share PHI without individual consent.[106] However, it is similar to many online health service rules which require an individual to authorize the site to allow another individual or healthcare entity access to the PHI.[107]

This bill allows the use and disclosure of EHRs in two situations. First is for primary uses, which are "use[s] for purposes of the individual's self-care or care by healthcare professionals."[108] HIPAA allows a similar use or disclosure of PHI for treatment or healthcare operations.[109] The participant maintains the EHRs for all primary uses but can authorize other entities (besides the IHRT operator) to retrieve or update information in the IHRT.[110] This is similar to an aspect of online health services which allows an individual to grant health entities access to PHI.[111]

---

standards of use of information to "provide a better user experience and to improve the quality of our services."), *and* Google Privacy Policy, http://www.google.com/privacypolicy.html (last visited Dec. 20, 2009) (indicating a good faith standard is applied when use of information is necessary to comply with the law).

105 H.R. 2991 § 5(a)(1).

106 45 C.F.R. §§ 164.506–164.508 (2009).

107 The individual decides with whom and which services they will share their information with. Additionally, Google will not share the information with other entities without the user's consent, except in limited instances such as when required by law. Google.com, Google Health Privacy Policy, http://www.google.com/intl/en-US/health/privacy.html (last visited Dec. 20, 2009).

108 H.R. 2991 § 6(a)(1)(B).

109 45 C.F.R. § 164.502(a)(1)(ii) (2008). Treatment is the "provision, coordination, or management of healthcare and related services by one or more healthcare providers[;] . . . consultation between healthcare providers relating to a patient; or the referral of a patient for healthcare from one healthcare provider to another." 45 C.F.R. § 164.501 (2008). Healthcare operations include activities of the covered entity that relate to covered functions, including: quality assessment and improvement activities; competency assurance activities; conducting or arranging for medical reviews, audits, or legal services; specified insurance functions; business planning, development, management, and administration; and business management and general administrative activities of the entity. *Id.*

110 H.R. 2991 §§ 6(a)(2)(A)(i), (B)(i)(I).

111 *See* HealthVault.com, Microsoft HealthVault Privacy Statement, https://

The second situation is for secondary uses. Secondary uses include "use[s] for purposes of public health research or other related activities."[112] Under this bill, an IHRT operator may sell the record or pieces of information from the record when the IHRT participant authorizes the information transfer.[113] The agreement between participant and operator must comply with the privacy protection agreement so that the participant is still protected.[114] The entity that receives the transfer of information must not further transfer the information to another entity or individual.[115] If this happens, the entity will be in violation of the agreement and will be subject to penalties.[116] HIPAA allows a similar use or disclosure for public interest and benefit activities.[117] Online health services also use and disclose PHI for statistical use, but the information is kept anonymous.[118]

B. Technologies for Restoring Users' Security and Trust (TRUST) in Health Information Act of 2008

One of the most promising bills that could potentially regulate online health services is the Technologies for Restoring Users' Security and Trust ("TRUST") in Health Information Act of

account.healthvault.com/help.aspx?topicid=PrivacyPolicy (last visited Dec. 4, 2009) (stating that individuals can decide with whom they want to share information with, such as to consult with their healthcare provider).

112 H.R. 2991 § 6(a)(1)(C).

113 § 6(a)(3)(A)(i).

114 In addition, the agreement must include "the parameters with respect to the disclosure of information involved . . . ." § 6(a)(3)(A)(ii). Further, the information the participant authorizes to disclose must be for research purposes only and the transfer must comply with Federal Trade Commission requirements and standards. §§ 6(a)(3)(A)(iii), (v).

115 § 6(a)(3)(A)(iv).

116 *See Id.* §§ 5(a)(1), 6(a)(3)(A(iv). Penalties include "(A) Loss of certification of the IHRT. (B) A fine that is not in excess of $50,000. (C) A term of imprisonment for the individuals involved of not more than 5 years." *Id.* § 5(a)(2).

117 *See* 45 CFR § 164.512 (2009) (allowing for the use and disclosure of personal health information for public health activities, including, but not limited to the collection of information for the "purpose of preventing or controlling disease," and for the "appropriate oversight of: [t]he healthcare system [and] [g]overnment benefit programs for which health information is relevant . . . .").

118 *See* Google.com, *Google Health Privacy Policy*, http://www.google.com/intl/en-US/health/privacy.html (last visited Dec. 20, 2009) (indicating data used in the trend statistics and associations will not be personally identifying information).

2008.[119] This bill aims to promote a national interoperable health information infrastructure that ensures personal privacy, security, and confidentiality with respect to PHI by regulating the uses and disclosures of PHI by qualified health information technology systems.[120] In addition, this bill aims to establish "minimum standards for the use and disclosure of individuals' personal health information and . . . promulgate regulations relating to personal health information that are consistent with individuals' right to privacy, security, and confidentiality with respect to the electronic use or disclosure of their personal health information . . . ."[121]

In order to be a "qualified health information technology system," the system would have to comply with seven requirements.[122] The first requirement is that the system "safeguards the privacy, security, and confidentiality of personal health information."[123] Online health services would have to comply with the privacy rights and security obligations of this bill.[124] The only privacy right for individuals currently not addressed by online health services is the right to receive notifications of suspected or actual security breaches of PHI. [125] Instead, the online health services suggest that individuals who notice a security breach inform the service.[126] The qualified health information technology system also has security obligations to the individual.[127]

---

[119] H.R. 5442, 110th Cong. (2d Sess. 2008) (as referred to the House Subcomm. on Health, Labor, Employment, and Pensions, April 17, 2008). No action has been taken on this bill since then.

[120] *Id.*

[121] *Id.* § 2(a)(13).

[122] § 213.

[123] § 213(1).

[124] These rights include: not having PHI disclosed without consent; inspecting and copying PHI; correcting or removing PHI; prohibiting anyone or any entity from viewing PHI; receiving notifications of suspected or actual security breaches of PHI; and receiving an accounting or all electronic disclosures of PHI upon request. H.R. 5442 §100.

[125] § 113(a).

[126] *See* HealthVault.com, Microsoft HealthVault Privacy Statement, https://account.healthvault.com/help.aspx?topicid=PrivacyPolicy (last visited Dec. 20, 2009) (encouraging individuals to contact the service if the individual feels that a program is not protecting their healthcare privacy and security).

[127] These obligations include: recognizing the individual's privacy; permitting individuals to inspect and copy their own PHI; providing notification of privacy practices to the individual; notifying individuals of suspected or actual security breaches of PHI; establishing and maintaining safeguards to ensure the privacy, security, and confidentiality of PHI; making a list of all data partners

The second requirement is that the qualified health information technology system "maintain[] and provide[] permitted access to health information in an electronic format."[128] Online health services provide PHRs to individuals in an electronic format.[129] However, individuals are responsible for maintaining and controlling access to the records.[130]

Qualified health information technology systems must also "preserve[] an audit trail of each individual that has gained access to" a PHR.[131] Online health services allow individual users to track entities that have access to their PHRs.[132] Google Health maintains a list of individuals and healthcare entities that have access to an individual's PHR.[133] However, Google Health does not appear to maintain an audit trail which can alert individuals as to when others are viewing theirs PHRs.[134]

A fourth requirement of a qualified health information technology system under this bill is for a system to "incorporate[] decision support to reduce medical errors and enhance healthcare quality."[135] Because online health services are not involved in the healthcare process, they would not meet this requirement. And since the seven requirements under this section are inclusive, an online health service is not a qualified health information technology system.

The fifth requirement of a qualified health information technology system is that it complies with this bill's section regulating healthcare improvement.[136] Online health services

with which the individual has contracted regarding PHI; obtaining an individual's informed consent before disclosing PHI; establishing and updating risk management procedures to protect against any breaches of PHI; establishing and maintaining a record of all PHI disclosures; and providing individuals with comprehensive information for any use or disclosure of PHI for marketing purposes. H.R. 5442 §100.

128 § 213(2).

129 *Id.* (recognizing that online health services provide electronic access to health information).

130 §§ 111(a)(1)-(5) (noting that individuals have the right to limit the use of their personal health information).

131 § 213(3).

132 Google.com, *Google Health Privacy Policy*, http://www.google.com/intl/en-US/health/privacy.html (last visited Dec. 20, 2009).

133 *Id.*

134 *See generally id.* (making no mention of the storage of information relevant to an audit trail, such as time of access, while indicating individuals may view what entities have viewed their PHR and block them from continuing to doing so).

135 H.R. 5442. 110th Cong. § 213(4) (2008).

136 § 213(5).

would have to become members of a "public-private Partnership for Healthcare Improvement."[137] Members include healthcare providers, health plans, "organizations with expertise in security; . . . [or] information technology vendors."[138] An online health service could be a member of the Partnership as a representative of either an organization with expertise in security, or an information technology vendor.

Sixth, a qualified health information technology system has to be able to "transmit and exchange information to other health information technology systems and . . . public health information technology systems."[139] Individuals and online health services do not transmit or exchange information with other systems. Rather, other entities are permitted to view health records only with the individual's consent. Online health services do not meet this requirement and they would not be considered qualified health information technology systems for purposes of this bill.

The final requirement is that the system "allow[] for the reporting of quality measures" in compliance with the bill.[140] The bill requires that PHI be collected "for the purpose of measuring the quality and efficiency of healthcare that patients receive."[141] Online health services post on their websites that they will disclose user PHI when required by law.[142]

C. Proposed State Legislation

In addition to proposed federal legislation, some states have recognized the need for better protection for individual PHI that is electronically stored. Several states are trying to enact legislation that establishes an individual's right to privacy regarding PHI.[143] In New Hampshire, a recent bill was proposed

137 § 202(a)(1).

138 § 202(b)(1)(A)(vi)(III)-(VI).

139 § 213(6).

140 § 213(7).

141 § 221(a).

142 HealthVault.com, Microsoft HealthVault Account Privacy Statement, https://account.healthvault.com/help.aspx?topicid=PrivacyPolicy (last visited Dec. 20, 2009). Microsoft will also disclose user PHI to "protect and defend the rights or property of Microsoft . . . [or] to protect the personal safety and welfare of users of Microsoft services . . . ." *Id.*

143 *See, e.g.*, H.B. 1587-FN, 160th Gen. Ct., Reg. Sess. (N.H. 2008), *available at* http://www.gencourt.state.nh.us/legislation/2008/hb1587.html; *see also* H.B. A06407, 232d Gen. Assem., Reg. Sess. (N.Y. 2009) *available at* http://assembly.state.ny.us/leg/?bn=A06407.

that "seeks to develop state privacy rules reaching further than HIPAA and pertaining to all entities handling health information, not just those HIPAA names."[144] The bill, if passed, would establish privacy rights for PHI that is in the possession of a healthcare provider.[145] Healthcare providers are defined as, in addition to the definition offered in HIPAA, "any person, corporation, facility, or institution either licensed by this state or otherwise lawfully providing healthcare services."[146]

Under this bill, an individual has the right to obtain an audit trail from the healthcare provider documenting all disclosures of that individual's PHI within the past three years.[147] HIPAA does not provide an individual with the ability to track who has been accessing the individual's PHI. In addition to an audit trail, an individual may restrict disclosure of PHI.[148] The healthcare provider must inform the individual that he or she has the right to restrict disclosure of PHI.[149]

The healthcare provider may disclose an individual's PHI "for treatment of the individual, for payment for services rendered to the individual, or for the healthcare provider's essential healthcare operations."[150] This is identical to one of the situations where a covered entity can disclose information under the HIPAA Privacy Rule.[151] However, this is the only situation under the New Hampshire bill where a healthcare provider may disclose an individual's PHI *without authorization*.[152] Normally, healthcare providers must obtain authorization from the individual in order to disclose PHI to an insurance issuer or a pharmacist.[153] However, healthcare providers are required to

144 Victoria Guay, Editorial, *Health Records Privacy Rules May Get Tighter*, http://www.citizen.com/apps/pbcs.dll/article?AID=/20080210/GJNEWS_01/67136800 (last visited Dec. 20, 2009).

145 *See generally* H.B. 1587-FN.

146 § 332-I:2(V).

147 § 332-I:3(III); *see also* § 332-I:2(II) ("'Audit trail' means a chronological record identifying specific persons who have accessed an electronic medical record, the date and time the record was accessed, and, if such information is available, the area of the record that was accessed.").

148 § 332-I:3(IV).

149 § 332-I:4(III).

150 § 332-I:4(I).

151 U.S. Dep't of Health and Hum. Services, *Summary of the HIPAA Privacy Rules*, http://hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (last visited Dec. 20, 2009).

152 *See* H.B. 1587 §332-I:4(IV) ; *see also id.* §332-I:5(I) ; *id.* §332-I:8.

153 § 332-I:4(IV)(a), (b).

provide the State with PHI when required by law.[154]

Under the New Hampshire bill, if a healthcare provider discloses PHI in violation of the bill it must inform the individual of the disclosure.[155] The New Hampshire bill goes beyond the HIPAA Privacy Rule to grant individuals more rights regarding PHI; however it only refers to healthcare providers and does not seem to include online health services. The New Hampshire Bill was sent to the House Committee on Health, Human Services, and Elderly Affairs for an interim study in April of 2008 and by October had been recommended for legislation, but no action has been taken.[156]

In addition to this bill, some states are trying to enact similar legislation that would advance the use of "interoperable electronic health records system[s]."[157] For example, Iowa passed a bill in 2008 which will organize a state-wide health information technology system by mid-2009.[158] This system would allow easier access to and compilation of health records for Iowa residents. One of the goals of Iowa's health information technology system is to "[p]rotect the privacy of consumers and the security and confidentiality of all health information."[159]

In Minnesota, many state employees will be able to access their PHRs online by the end of 2009.[160] In addition to the access to PHRs online, the state employees will be able to seek treatment options and use a "flexible spending account debit card to pay for eligible out-of-pocket costs."[161] The Minnesota Governor plans to make online PHRs available to all Minnesotans by 2011.[162]

Even New York City is attempting to convert PHRs into electronic format.[163] The city is offering doctors, especially those

154 § 332-I:4(IV)(c).

155 § 332-I:8.

156 The New Hampshire General Court, Bill Status System, http://www.gencourt.state.nh.us/bill_status/bill_docket.aspx?lsr=2417&sy=2008&sortoption=&txtsessionyear=2008&q=1 (last visited Dec. 20, 2009).

157 H.F. 82-2359, 82d Gen. Assem. §25.135.156.1(a) (Ia. 2008); *see also* Minn. Stat. § 62J.495 (Mn. 2008).

158 H.F. 82-2359 §25(3).

159 § 24(2)(c).

160 Posting of Jacob Goldstein to Wall St. J. Health Blog, http://blogs.wsj.com/health/2008/07/30/minnesota-governor-wants-online-health-records-for-all/ (Jul. 30, 2008, 09:36 EST).

161 Lopez, *supra* note 4, at 1.

162 *Id.*

163 Posting of Jacob Goldstein to Wall St. J. Health Blog, http://blogs.wsj.com/health/2008/12/30/new-york-citys-60-million-push-for-electronic-medical-records/ (Dec. 12, 2008).

in small practices, subsidies if they agree to convert patient records to electronic form and participate in a program that will rate city doctors.[164]

> New York is trying to connect the vast majority of medical practices, which have 10 or fewer doctors, particularly in poorer neighborhoods, in hopes that providing them access to a broader base of patient information—and ranking their performance against their peers—will help them make strides in *preventive medicine*.[165]

A similar program is being tested in Massachusetts by the eHealth Collaborative, which links the medical records of three suburban and rural communities.[166]

V. RECOMMENDATIONS

With governmental encouragement to convert medical records to EHRs, online health services like Google Health and HealthVault provide individuals with an easy way to store and manage their EHRs. The economic stimulus bill proposes to fund the use of EHRs but has not proposed any means of safeguarding the EHRs themselves. If Congress wants to have a successful transition from paper records to EHRs, there should be more research into viable technologies to store, manage, and safeguard EHRs, thereby protecting an individual's PHI.

Online health services have fallen into a gap in legislation regulating the privacy and security of individual electronic PHI. Because they are not covered under the HIPAA Privacy Rule, they are not subject to the Privacy Rule's sanctions if an individual's privacy is compromised. Additionally, online health services fall outside of the scope of recent proposed federal and state legislation and would not be subject to their sanctions. Most of the bills, both at the federal and state level, focus on health entities that provide healthcare services. In order to regulate online health services, these bills must include entities that merely *store* health information, rather than entities that transfer health information.

The federal bills do not specifically incorporate online health services into their definitions of IHRTs or qualified health

---

164 *Id.*

165 Anemona Hartocollis, *City to Pay Doctors to Contribute to Database*, N.Y. TIMES, Dec. 30, 2008, at A19, *available at* http://www.nytimes.com/2008/12/30/nyregion/30records.html?_r=1&partner=permalink&exprod=permalink.

166 *Id.*

information technology systems. Online health services seem to almost fit the description of an IHRT. But legislators would have to specifically incorporate online health services into this bill. Therefore, my first recommendation would be to change the language of proposed legislation to include online health services as entities covered by federal legislation and subject to the same standards of privacy and security as HIPAA covered entities. For example, the bill should include language like "electronic storage facilities of PHI" when discussing IHRTs. This would incorporate online health services and treat the service companies (like Google and Microsoft) as IHRT operators, thus requiring the companies to comply with the fiduciary duties of an IHRT operator.

The most promising piece of legislation regarding regulation of online health services is the TRUST in Health Information Act of 2008. If the requirements for qualified health technology systems would be changed from an inclusive standard to a less restrictive standard, online health services would meet the requirements of a qualified health information technology system. Online health services comply with five of the seven requirements in order to be defined as a qualified health information technology system. The rigidity of the definition of a qualified health information technology system keeps an online health service from being a "covered entity."[167] Therefore, online health services like Google Health and HealthVault will fall outside of the scope of this bill.

A change in the language of the bill to make the definition of a qualified health technology system less restrictive would allow for government regulation of online health services. Further, online health services would be subject to federal penalties if a breach or unauthorized disclosure of PHI occurs. By including online health services into federally regulated health information entities, people who use these services will be afforded greater security and privacy protections because the services will have to comply with the minimum safeguards that the federal regulations promulgate. Changing the language of the federal bills and enacting them into legislation would close the gap that keeps online health services from being regulated by federal laws.

Another example is the New Hampshire bill, which is very

167 *See* H.R. 5442, 110th Cong. § 213 (2008).

similar to HIPAA regarding the covered entities even though the purpose of the bill claims to incorporate more entities than just those covered by HIPAA. But here too the definition of a healthcare provider under the New Hampshire bill precludes online health services because they do not provide healthcare services.[168] Therefore, under this bill, online health services like Google Health and HealthVault would still not be subjected to any sanctions if they violate an individual's right to privacy regarding their PHI. To be more effective at regulating electronically stored PHI, New Hampshire should include online health services in its definition of healthcare entities by defining them as electronic storage facilities of individual PHI. This inclusion would hold online health services to the same standards of privacy and security as covered healthcare entities.

My second recommendation would be to incorporate online health services under a federal standard of privacy and security regarding EHRs. While state legislators, such as those in New Hampshire, are also trying to form legislation that would protect the privacy and security of individual PHI, a federal statute, similar to HIPAA, would be more beneficial. Under a federal statute, there would be a nationwide standard for privacy and security, making it easier for online health services to comply with one law, rather than the laws of each state. Some states, like Iowa and Minnesota, have already begun implementing a statewide online health information technology system that would make maintenance of PHI easier for individuals residing in those states. Additionally, cities and counties in other states are starting to implement similar systems. While having these systems will provide an individual with easier access and maintenance of records, it will be difficult if that individual wishes to transfer records from another state or city that either does not have an online health information technology system or a system that is not compatible with the individual's home system. A nationwide online health information technology system would alleviate any problems transferring records to another state.

A third recommendation would be to look into alternative methods to keep EHRs secure. In addition to explicitly including online health services into the category of federally regulated

[168] H.B. 1587-FN,160th Gen. Ct., Reg. Sess. § 332-I:2(V) (N.H. 2008) *available at* http://www.gencourt.state.nh.us/legislation/2008/hb1587.html.

health information entities, legislators should be looking at other ways to protect an individual's electronic health information. For example, a Rand Corporation study "suggests that it's easier to safeguard patient privacy with a records system that makes use of a unique health ID rather than a system that uses statistical matching."[169] Statistical matching takes personal information, such as a name, address, birth date, or Social Security number, to match an individual with test results and medical history.[170] However, this system is more likely to produce errors, including linking to the wrong patient's records and identity and medical identity theft. With a unique health ID number, none of the individual's personal information is available so there is less of a chance of any form of identity theft. In addition to PHI security and privacy, implementing a nationwide unique health ID number for all American citizens will cost approximately $11 billion,[171] but could wind up saving the government almost "$77 billion in increased efficiency and reduced errors."[172]

A final recommendation would be to publicly display a list of HIPAA covered entities and online health services that have breached the privacy and security of an individual's PHI. In the TRUST in Health Information Act of 2008, the bill proposes that the Secretary of Health and Human Services maintain this list, which would be available to the public.[173] The list "shall . . . identify[] health information persons that have lost, stolen, disclosed, or used in an unauthorized manner or for an unauthorized purpose the personal health information of 1,000 or more individuals."[174] While the bill proposes that the list reveal

169 Press Release, Rand Corporation, Creating Unique Health ID Numbers Would Facilitate Improved Healthcare Quality and Efficiency (Oct. 20, 2008) *available at* http://www.rand.org/news/press/2008/10/20/; *see also* Posting of Susan Brink to The L.A. Times Health Blog, http://latimesblogs.latimes.com/booster_shots/2008/10/your-own-health.html (Oct. 20, 2008 , 3:57 PST).

170 Posting of Susan Brink to the L.A. Times Health Blog, http://latimesblogs.latimes.com/booster_shots/2008/10/your-own-health.html (Oct. 20, 2008, 3:57 PST).

171 RICHARD HILLESTAD,ET AL., IDENTITY CRISIS: AN EXAMINATION OF THE COSTS AND BENEFITS OF A UNIQUE PATIENT IDENTIFIER FOR THE U.S. HEALTHCARE SYSTEM 31 (2008), *available at* http://www.rand.org/pubs/monographs/2008/RAND_MG753.pdf.

172 Posting of Susan Brink to the L.A. Times Health Blog, http://latimes blogs.latimes.com/booster_shots/2008/10/your-own-health.html (Oct. 20, 2008, 3:57 PST); *see also* HILLESTAD, *supra* note 171, at xviii.

173 H.R. 5442, 110th Cong. § 114(c) (2d Sess. 2008).

174 *Id.*

the number of individuals affected,[175] the list should also include the type of breach committed by the entity or service. Such a list would be beneficial for the public so an individual can make an informed decision about using certain online health services to maintain PHI.

The government at both the Federal and State level recognize the need to safeguard EHRs. If the federal government proposes legislation that would regulate online health services that store individual PHRs electronically and incorporate a unique health identifier for American citizens, an individual's PHI will be better protected.

[175] *Id.*