The World Privacy Forum

A Legal and Policy Analysis

Personal Health Records: Why Many PHRs Threaten Privacy

Prepared by Robert Gellman for the World Privacy Forum

February 20, 2008

About this Analysis:

This document offers a legal and policy analysis of the privacy consequences for consumer health information stored on or by Personal Health Records systems that are not subject to the HIPAA health privacy rule. This document does not analyze the potential of PHRs for affecting the cost of health care in general. Unless specifically noted in the text, the term PHR in this document refers to PHR records and systems that are not subject to HIPAA.

Summary:

Personal health records (PHRs) are touted as a new convenience technology for consumers. However, some PHRs can have significant negative consequences for the privacy of consumers who authorize the maintenance of their health records by PHR vendors. Federal rules for health providers and insurers do not protect records maintained by many PHR vendors. This analysis focuses mostly on those PHRs that are not covered by the federal HIPAA health privacy and security rule.

Significant privacy consequences of PHRs not covered under HIPAA can include:

- Health records in a PHR may lose their privileged status.
- PHR records can be more easily subpoenaed by a third party than health records covered under HIPAA.
- Identifiable health information may leak out of a PHR into the marketing system or to commercial data brokers.
- In some cases, the information in a non-HIPAA covered PHR may be sold, rented, or otherwise shared.
- It may be easier for consumers to accidentally or casually authorize the sharing of records in a PHR.
- Consumers may think they have more control over the disclosure of PHR records than they actually do.
- The linkage of PHR records from different sources may be embarrassing, cause family problems, or have other unexpected consequences.
- Privacy protections offered by PHR vendors may be weaker than consumers expect and may be subject to change without notice or consumer consent.

About the World Privacy Forum:

The World Privacy Forum is a non-profit public interest research and consumer education group. It focuses on in-depth research and analysis of privacy issues with a particular focus on issues relating to the health care, financial, and technology sectors. The World Privacy Forum was founded in 2003.

Personal Health Records: Why Many PHRs Threaten Privacy

I. Introduction

Personal health records – or PHRs – are a relatively new phenomenon in health care today. As discussed here, a PHR is 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. Businesses large and small are moving to take advantage of the potentially lucrative new business model PHRs provide, especially as leveraged through the Internet. Some of the newest PHR players include large and well-known technology companies, but some health care providers, insurers, and employers also promote PHRs. There are dozens of different PHR vendors.

As a new type of convenience technology for consumers, PHRs are promoted as giving consumers more knowledge and an opportunity to be more actively engaged in their own health care. Physicians, insurers, laboratories, and others who create or handle a consumer's health care records can deposit copies of records in the consumer's PHR. A consumer can also put information in his or her PHR, depending on the PHR system.

One alleged promise of PHRs is that consumers will have more control over their own health care because their information will be more accessible to them. PHRs may offer some benefits for consumers, but there are also potential negative consequences both for consumers and for the health care system at large that have not been carefully examined. It is crucial for consumers to understand the potential privacy consequences that exist before they share sensitive health information outside the health care system.

The role of HIPAA in PHRs

Not all PHRs have equal privacy protections. Some PHRs operate within the health care system and are covered under HIPAA. But some PHRs operate outside of HIPAA, and this is a point of confusion for many consumers.

HIPAA is a federal rule that establishes a baseline for health privacy in the United States. The HIPAA acronym stands for the *Health Insurance Portability and Accountability Act*. Under the authority of that Act, the Federal Department of Health and Human Services issued a health privacy rule and a security rule. These rules establish minimum privacy and security standards for *covered entities*. A covered entity is a health care provider, health insurer, or clearinghouse.

Because of the structure of HIPAA, its privacy protections do not generally follow a health record. The applicability of HIPAA's privacy protections depends on the kind of entity that processes a health care record. The basic idea is that if a health care provider (hospital,

physician, pharmacist, etc.) or a health plan maintains a health care record, the record is protected under HIPAA. However, if a person or business that is *not* a covered entity under HIPAA holds the records, then HIPAA does not apply. This is a highly simplified description of a complicated rule.

For PHRs, the important thing is that **unless the PHR vendor is itself a covered entity under HIPAA, the HIPAA health privacy rule does not apply**. Even if a covered entity sponsors a PHR, it is still possible that the HIPAA privacy protections will not apply, depending on the circumstances. Many PHRs that have come to public attention are commercial and fall outside of HIPAA.

PHR business models

A variety of intricate business models exists in the PHR world. There are generally three types of commercial PHR business models. In one model, a consumer simply pays for the PHR service. In a second model, a PHR is free to consumers because the service is supported by advertising. In a third model, an employer or health plan might pay for the service, perhaps with the hope of saving money on health care costs. All three funding models could be in play at the same time. For example, a PHR service paid for by an employer, health plan, or consumer may still sell advertising.

It should be noted that in these models, many other technology elements may be present. There may be informational web sites, niche search engines, articles, surveys, software downloads, and a host of other offerings (or not) associated with the PHR system. No matter what the configuration, the pressure to make a profit can place commercial PHRs in conflict with consumers over privacy.

A physician is bound by law and medical ethics to not exploit patient records for personal profit. However, the commercial variety of PHRs not covered under HIPAA generally do not operate under the same legal and ethical traditions. They may not be bound by laws established for the health care sector or by any established medical ethical guidance.

Risk of consumer confusion

Few consumers understand the complex workings of HIPAA. It has always been important for consumers to understand the broad outlines of HIPAA, and especially to understand their rights under HIPAA. But the need for clear consumer understanding has greatly increased due to the high potential for confusion the PHR trend has raised.

This interplay of "is it covered under HIPAA? Is it not covered under HIPAA?" is where the risk of consumer confusion is highest. Consumers may assume that a health care record has special protections in its own right, because this is what they are used to at their doctor's office. But as discussed, this is not how the federal HIPAA health privacy protection works. HIPAA will not

apply to many commercial PHRs, and many state health privacy laws will not apply either. But how many consumers know this?

II. Discussion

The HIPAA privacy rule provides a degree of privacy protection for covered health records. The rule has problems and gaps, but it does establish minimum national privacy standards for disclosure, access, correction, and other elements of fair information practices. State laws that provide additional privacy protections remain in effect and can provide additional legal protections for privacy.

Comparing the privacy of PHR records outside of HIPAA to records held under HIPAA shows how the two regimes of protection compare. For the most part, the privacy of any PHR records not covered under HIPAA necessarily falls short of the HIPAA standard. Key areas of concern are privilege, subpoenas, marketing of health care data, linkage of records, security, ability to correct files, consent issues, and the role of privacy policies.

PHRs and Privilege

Many people are aware that health information may be privileged, but few – including some physicians – fully understand what that means. The physician-patient privilege (and the sometimes separate psychotherapist-patient privilege) offers some protections for confidential communications between physician and patient.

The privilege is statutory, is of limited utility, is not always available, and has extensive exceptions. This is not the place to discuss the complex legal details. When privilege does apply, the privilege can prevent a physician from disclosing a confidential communication with a patient. The privilege provides a significant privacy protection when it is available.

One basic requirement is that the privilege generally only applies when a communication is truly confidential and between physician and patient only. Traditionally, if a spouse or a nurse is present at the time of the communication, the privilege does not apply. Some statutes maintain the privilege even when a spouse or nurse is present, however.

What happens to the privilege when a consumer instructs her physician to send a copy of a health record to a commercial PHR company? Because PHRs are new, and there has been no reported litigation, the answer to this question is uncertain. However, it is seems certain that a prosecutor or another person who wants a consumer's health record will argue that the consumer waived any privilege by sharing the record with a third party. A court is likely to agree that the patient waived the privilege by consenting to the disclosure.

Use of a PHR by a consumer on an office computer or other employer-owned Internet access device may also affect the privileged status of health information. Most employers reserve the

right to read electronic mail sent over an employer's network, and the exposure of electronic mail to the employer could undermine any privilege. The same may be true for any other use of an employer's computer facilities, including use of an office computer to read or add information to a PHR. Employers may reserve the right to review all activities on their computer facilities, including using keystroke loggers and other tracking techniques. That kind of review may undermine the privilege of any health information that passes over an employer's system, whether between employee and physician or between employee and PHR.

At a minimum, the consensual sharing of a record with a commercial PHR vendor will not enhance the record's privilege, and it could defeat the privilege altogether. This is not a trivial issue, and it is one that could come as a surprise to many consumers and health care providers.

PHRs and Subpoenas

Health records, like just about any other record containing personal information held by a third party, can be subpoenaed under a variety of circumstances. For example, a consumer's records could be sought in a tort suit (e.g., auto accident or medical malpractice), in a divorce or other family lawsuit, or sought if the records are relevant to someone else's lawsuit. The rules governing subpoenas for health records are complex, and HIPAA includes some significant procedural protections.

In general – noting that there are some exceptions that are too complicated to list in the context of this analysis – if someone seeks to subpoena health records about a consumer from a covered entity, HIPAA requires the person seeking the records provide notice to the consumer. With that notice, the consumer has the chance to contest the subpoena, to argue that the request is too broad, to object that the records are not relevant, or to seek a protective order.

Unfortunately, the protections covering subpoenas of health records provided by HIPAA will not apply to PHRs (unless a covered entity operates the PHR). As a result, no law requires that a consumer receive a notice of a subpoena served on the PHR. Thus, the records in a non-HIPAA-covered PHR do not have the basic procedural protection provided by HIPAA for subpoenas. A non-HIPAA covered PHR company could potentially establish a privacy policy that requires it to give its customers notice of a subpoena, but a privacy policy can be changed at any time.

Another issue is that if a lawyer has a choice between subpoenaing a record from a physician or from a PHR vendor, the lawyer may find it easier to go to the PHR vendor. The PHR record may be centralized, include records from several providers, and be electronic -- all features facilitating the sharing and the utility of the records. The PHR record may not always be as useful legally as the original physician's record, however.

Still, notice for the subpoena is not a legal requirement for non-HIPAA covered PHRs, and the lawyer seeking the record does not have to worry that the physician will claim privilege or otherwise resist the subpoena. A health care provider may perceive a legal, ethical, or professional responsibility to protect a patient's health record and resist a subpoena. A PHR vendor may have none of those responsibilities and is not likely to be willing to expend funds

fighting subpoenas on behalf of a consumer. Some commercial PHR vendors may be willing to provide notice to a consumer even if not legally required, and a commitment to that effect is noteworthy.

PHRs and Marketing

Perhaps the biggest single concern about commercial PHRs is the possibility that a consumer's health information will leak into the marketing system. The terms under which a PHR operates could allow the sale or rental of consumer information in the same way that magazines, catalog companies, magazines, charities, or other merchants and activities share information with limited or no consumer knowledge or consent. Consumers generally have some sense about how readily companies and agencies pass personal information around, but they do not expect the same kind of sharing when it comes to personal health information.

HIPAA generally prevents use or disclosure of health information for marketing purposes. There are a few mostly unremarkable exceptions to the marketing prohibition, and some definitional issues cloud the picture. Nevertheless, the HIPAA marketing prohibition mostly mirrors what people expect. Physicians' ethics prevent them from selling lists of identifiable patients to pharmaceutical manufacturers or to markets, and the HIPAA rule makes those sales legally improper.

However, the marketing prohibitions of HIPAA do not apply to PHRs that are not offered by covered entities. A 2007 study of PHR privacy policies conducted for the Department of Health and Human Services found that only 3 percent, or one in 30, of PHR privacy policies stated that explicit consumer consent was necessary prior to the vendor sharing any of the data in the PHR (See R. Lecker et al, *Review of Personal Health Record (PHR) Service Provider Market*, Jan. 5 2007 at 7. http://www.hhs.gov/healthit/ahic/materials/01_07/ce/PrivacyReview.pdf). Meanwhile, none of the PHR privacy policies analyzed in the study expressly named the PHR vendor's data partners, third parties, or other secondary uses of the PHR data, or whether the data was de-identified or not. Even if a PHR vendor states that it does not share information with marketers without consent, it may be still be easy for the vendor to induce consumers to give consent without actually realizing what they are doing.

Why would a PHR vendor want to disclose information for marketing purposes? The answer is simple: money. Many PHRs are free to consumers. Who is paying for the service? In some cases, it might be an employer or health plan. However, for other PHRs, marketing and advertising are the only or the primary sources of revenue. Under those conditions, commercial PHR companies can find many ways to share consumer information with marketers. The extensive sharing of consumer information – whether identifiable or not – is a standard revenue source for many Internet activities.

One example of the demand for patient information may be seen by looking at pharmaceutical manufacturers. These companies generally do not know who their customers are. They cannot find out because medical ethics and HIPAA prevent doctors and pharmacists from sharing the names of those who have prescriptions. The manufacturers work hard to find information

through other methods. They want to know who uses their drugs and who uses a competitor's drug. To find out, the companies may offer coupons for free or discounted medicine that requires consumers to provide names and addresses. Companies may offer magazines for people who have a particular disease. They may have toll-free numbers for people to call. Companies may also use websites to obtain the names and survey information from consumers. Any information that manufacturers obtain – or any other marketers for that matter – is theirs to keep, use, and disclose as they please because no American privacy law typically applies.

Even if a PHR vendor solemnly swears that it will not provide consumer information to marketers, any PHR that allows advertising on its website may facilitate the disclosure of the information anyway. Here's a scenario that may apply in some cases. Let's assume that advertisers want to place their ads where it will do the most good. For example, a company advertising birth control pills will not pay to place its ads where men will see them. The PHR vendor can make sure that the ad only appears on pages viewed by women, and it can do so without disclosing any personal information about the women who see the ad. The advertiser knows that anyone who saw the ad or clicked on it is registered on the website as a female.

A PHR vendor can target ads more narrowly so that they appear only to 50-plus year-old white males with diabetes, an annual income over $75,000, and a health plan that pays for drugs. The targeting itself may not disclose any personal information, depending on how it is done. However, when the user clicks on the ad, the advertiser can often infer that the user has certain the specified characteristics. If the advertiser can identify the user because of a previously set "cookie," because of the user's static IP address, because of another behavioral tracking activity, or because the user casually provides a name or email address to obtain more information, the specified information about the consumer can pass to a third party advertiser. The advertiser may then use the information, disclose it to others, share it with commercial data brokers, or do anything is pleases because no privacy law typically applies and because it is not typically subject to the PHR's privacy policy.

Regardless of the PHR's policy on marketing disclosures, advertising can provide a method for a consumer's health information to escape into marketing files. Marketers already have millions of names of consumers categorized by specific diseases and diagnoses. Most of the information comes from consumers who provided it in response to "consumer surveys" or through other stealthy methods for collecting health information for marketing use. Health records maintained by health care providers have been unavailable to marketers directly, but commercial PHRs operated outside of HIPAA offer marketers the promise of more and better health information from consumers.

Advertising-supported PHRs are not necessarily likely to support or allow strict control over consumer information or to fully and readily tell consumers how personal information may be shared. Many PHRs will only succeed if they can sell advertising, and advertisers will seek as much detailed information about PHR clients as they can obtain. Wheedling consent from consumers for the profitable sharing of records is something that some PHRs are likely to try. Casual clicks or agreements by consumers may release the health records they have uploaded irretrievably to marketers, data brokers, and others. Many consumers may not be aware of the

sophistication of how targeted marketing technologies and practices operate online or in other arenas.

The PHR as a Depository

Some PHRs present themselves as a depository of health information under the control of the consumer. The suggestion is that the records have inherent privacy protections because the consumer has some choices or control over the record, including who may see, add to, or change the record. By contrast, covered entities under HIPAA can disclose health records to many institutions for many purposes without consumer consent. That is one of the controversial aspects of HIPAA. HIPAA allows many disclosures without the consent of – and indeed over the objections of – the consumer.

Will a consumer-controlled health record deposited in a PHR add to or protect the privacy of the records? Nothing about the PHR changes the reality of health privacy protection, except that the information is now duplicated in a new location and subject to the rules of a new organization. No matter how much control a consumer may have over his or her PHR records, a PHR depository does nothing to improve the general privacy of health records. Even if the PHR's privacy and security controls work perfectly, the records now exist in one more location than before and may have additional vulnerabilities.

Suppose that a consumer has a totally secure safe in her home that can only be opened with her express approval. The consumer writes down her Social Security Number (SSN) on a piece of paper and puts that paper in the safe. Is her SSN more protected than before?

Not really. Everyone else who had the SSN before the paper was deposited in the safe still has it. That includes banks, the IRS, credit bureaus, employers, the Social Security Administration, a partner or spouse, and perhaps dozens of other agencies and organizations. The locked safe does nothing to enhance the privacy of the SSN, although the privacy and security of that one piece of paper may well be improved.

For health records, the information in the PHR must originate from somewhere. Prime sources are physicians and insurers, but in some PHRs consumers can also add information about their use of supplements, gyms, and so forth. The health information about consumers held by their physicians, health plans, dentists, laboratories, pharmacies, and others remains exactly where it was before it entered the PHR. That information is subject to the same good or bad rules or practices that applied before the deposit of the information in the PHR.

No one who had the ability to obtain health information before a copy entered the PHR need pay any attention to the PHR or any consumer controls on the PHR. The records that were available before from other sources remains available. For example, health fraud investigators can obtain patient records for their work. Putting a record in the PHR changes nothing because the fraud investigators can still obtain the record from the physician or health plan. The PHR record is *a* copy but not *the only* copy. Consumers who see the control promised by PHR vendors may be easily confused about the meaning of that control.

PHRs and Linkage

Some privacy protections exist because independent health care providers maintain separate records about consumers. A dentist has one set of records; a family doctor has another set. It will often be the case that the two sets of records are not linked or shared routinely. However, those who obtain health care from a single health maintenance organization may already have centralized records. Linkage of health records offers some advantages, but not all linkages are necessarily welcome to consumers.

A consumer may not care to let her dentist know that she is under psychiatric care. Another consumer will not want a health plan or employer to know about a genetic test paid for out-of-pocket. A third consumer may not want anyone to know that he sought treatment for a sexually transmitted disease. For good reasons or not, people may want to keep some of their health information strictly private, even within the health care community. Consider a college student who drank too much alcohol and ended up in the emergency room. Consider a soldier who visited a psychiatrist due to suicidal thoughts. Consider people who had a learning disability in their youth. Other sensitive conditions may include attention deficit disorder, weight problems, cosmetic surgery, bedwetting, and others. Many people have some information in their health records than they are not comfortable sharing with anyone, especially years later.

As time passes, as people move, and as people change physicians, older information tends to disappear, get lost, or remain disconnected from current information. That benefits privacy, although the loss of some old information may sometimes, but not always, negatively affect health care. PHRs may bring old information together in ways that may not please consumers all of the time.

When a consumer consents to place health information in a PHR, how much actual control will the consumer have over this kind of file linkage? A consumer may be willing to share information with one health care provider but not another. Another may not be willing to tell a spouse or other family member about some parts of a medical history. Suppose that a niece is looking after her aunt following hip-replacement surgery. The aunt may not want her to see the part of the record that revealed a history of alcoholism or drug abuse. Controlling disclosures of recorded health information can be complicated because consumers may be willing to share some information all of the time, all information some of the time, and other information never.

Does a PHR provide the tools that allow consumers make these decisions? It may not be enough if a consumer can only decide who can or cannot see a health record. A consumer may need to be able to exercise a finely granulated degree of control across time, people, and information. The sharing of information within a family and across generations may be especially complicated. Health records may reveal secret information not shared widely within a family, between parent and children, or between spouses. The disclosure of family medical secrets has the potential to poison relationships and undermine marriages.

HIPAA offers some controls over disclosure to family members and to caregivers. The HIPAA tools are not perfect, and much depends on how health care providers exercise the discretion that they have. However, relying on health professionals to make decisions about information disclosure may be more comforting than rules applied by a computer. Oral disclosures are more easily limited to current treatment information, and health care providers must accept direction from patients on family disclosures. Each PHR user must assess if a PHR provides the tools to keep health information out of unwanted hands and to put that information only into the right hands. An all-or-none approach to information sharing is not likely to meet everyone's needs.

Another type of health record linkage is likely to be refused by PHRs. Some records – principally those covering treatment for drug and alcohol abuse – have strong statutory protections that follow the record even when the consumer consents to the disclosure. The restrictions are strict, and it is possible that a PHR will refuse to accept information that comes with special privacy restrictions. The result may be that for some consumers, a PHR cannot even fulfill the promise of bringing all of the consumer's records in one place. Similar problems might arise with records about genetics, HIV/AIDS, and psychiatric treatment. Some physicians may also refuse to share records with a PHR, even if the consumer requests sharing. Any of these limitation may be a good thing or a bad thing, depending on a person's perspective and medical history.

Yet another type of linkage may happen if the PHR vendor also offers other Internet services. If the PHR vendor also has access to a consumer's email through an email service, to a consumer's documents through an online storage service, or to a consumer's Internet searches through a search service, the information that the PHR vendor collects through the consumer's use of the company's other online services could potentially be linked to the PHR record. Much will depend on how the company decides to link – or not – the data. The profiling of consumers through the Internet and other digitally intermediated activities is a major activity today, and the addition of health information to profiles could make the data even more valuable to marketers.

PHRs and Security

Security is an important part of privacy. Are PHR records more secure? The answer depends on who maintains the PHR and whether the security of the PHR is sufficient. Information held by health care vendors and insurers is subject to the HIPAA health record security rule. For what it is worth, the HIPAA security rule has attracted less criticism than the HIPAA privacy rule. Whether any given health record keeper is actually doing a good job of complying is hard to say.

But **-- the HIPAA security rule does not apply to a PHR vendor that is not a HIPAA covered entity.** The security a commercial PHR vendor supplies could be better than required by HIPAA, or it could be worse.

Can consumers trust big Internet or technology companies to protect health record security? It is clearly in the interest of these companies to protect their customers' records. Nevertheless, recent history is replete with examples of data breaches and security gaffes by big organizations with

sophisticated security mechanisms. Most software and operating systems in use today are significantly vulnerable to hackers and others.

In the end, however, even if protected by state-of-the-art technology, it is difficult to argue that a PHR vendor enhances the overall security of health information. At best, another organization that did not have the information before now maintains it in yet another location, whatever that configuration may be -- whether that be a networked database or otherwise. If the security is truly good, than a consumer may be no worse off than before. However, the 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.

PHRs and Correction

One basic privacy right is the right to seek correction of personal information that is incorrect or incomplete. This is a difficult area for health records because health care providers do not like to change records, and they strongly resist removing information from a record. Often, the resistance is reasonable. For example, a preliminary diagnosis may turn out to be wrong, but the record of the diagnosis must remain in the record to explain a particular test or treatment.

What rules apply to the correction of PHR records? Many records in PHRs may originate with a health care provider. Who can change or delete the records? Will a PHR vendor change records only with the consent of the health care provider who supplied the records or can the consumer who is the subject of the record change it? Just who actually controls the record?

If the consumer truly controls the PHR record, then the consumer should have correction rights. However, if the record is to be shared with other health care providers, those providers will be understandably reluctant to rely on records that the patient changed. What happens when providers disagree about a patient's diagnosis? Can one provider change another provider's record? Can the consumer change both records? Suppose that a consumer deleted evidence of a prescription for a controlled substance in the hopes of obtaining a duplicate prescription from another doctor.

Here's an example to illustrate a part of the problem. Suppose that a PHR record shows that John Doe had an appendectomy last year. However, this John Doe knows that he did not have the surgery. The record came from a surgeon who accidentally put the wrong patient number on it or who mixed up the record with another patient with the same name. Perhaps the PHR vendor matched records incorrectly. Another possible cause is a medical identity thief who obtained Doe's insurance number and used it to obtain treatment in Doe's name.

What can the consumer do about the incorrect information now in a PHR? HIPAA has some procedures for correction, but patient correction rights under HIPAA are inadequate in some circumstances. This is a messy area for all health records, but the centralization of records in a PHR may magnify some of the messy elements.

The principal difference between a HIPAA record and a non-HIPAA PHR record may be the issue of control. The health care provider controls the record maintained about a consumer's care, and the consumer must negotiate corrections with the provider. The correction rights available under HIPAA can help consumers, although they do not work perfectly. The PHR vendor may have obtained the record with consumer consent, but it may not be clear if the consumer will have the right or ability to change it, depending on the structure of the PHR system. If the PHR requires that the consumer correct the original physician record first, the result may be an administrative or legal nightmare. For example, a health care provider may be unwilling to correct the record, may not be required to do so under HIPAA, or may no longer be in practice. However, if the PHR allows the consumer to correct the record directly, the value of the records may be undermined.

Corrections of health records are complicated, and no existing set of rules works well in all circumstances. Putting health records in a PHR may make existing problems worse, and it will almost certainly be more complicated because of the presence of a new record keeper whose responsibilities may not be clear and who may not be trusted by health care providers.

PHRs and Consents for Disclosure

Under HIPAA, if a consumer wants to authorize a covered entity to disclose her records, she will usually be obliged to sign an authorization form. The HIPAA rule prescribes the content of the authorization form and its scope. That rule provides some protections because it makes it harder for a consumer to unknowingly sign a form authorizing the disclosure of health records. For example, if a consumer signs a one-sentence form authorizing anyone with records about the consumer to disclose the records to the bearer of the form, it is unlikely that any doctor or hospital would or should honor that form.

What rules apply to PHRs? Most existing laws about authorizing disclosures of health records predate PHRs, and few of those laws will apply. Unless a law applies, the PHR vendor sets the rules for the records it maintains. It can honor a one-sentence authorization form signed five years earlier. It can accept a tick box checked while reading an ad on the PHR website. Suppose, for example, that 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 (if there is a privacy policy). In the digital environment, consent can often amount to nothing more than a pre-checked box in small print at the bottom of a lengthy notice. It may be in the interest of the PHR company – but not the consumer – to readily allow disclosures in order to increase advertising revenues.

In the absence of law, a PHR can have any rule that it chooses about disclosing information with consent. It can require affirmative consent (opt-in) on a designated printed form. It can allow disclosure for some activities unless a consumer objects (opt-out) by submitting a letter through

postal mail. The PHR vendor can accept a checked box on a website. Whether a PHR's consent rules and procedures are adequate is for each consumer to evaluate. The process may vary from PHR to PHR and, perhaps, even within the same PHR system depending on the type of disclosure. Those who surf the web routinely know that it can be easy to check a box, forget to uncheck a box, or agree to something unintentionally because the authorization was buried deep in an unread notice. A casual consent to enter a sweepstakes for a one-in-a-million chance to win a t-shirt could obscure a broad authorization for the disclosure of health information. That type of authorization would not comply with HIPAA requirements, but a non-HIPAA covered PHR vendor could accept it.

Many organizations may want to use PHR records for other purposes. Finding old or scattered health records can be challenging in many cases. If the PHR vendor successfully gathers records from many sources, it will be a boon to those outside the health care system who want health information about consumers and have the leverage to obtain some form of consent. Why seek records in a dozen places when someone has nicely centralized them and can share them in digital formats? It is likely that PHR records will be sought by insurance companies for consumers who apply for life insurance or individually underwritten health insurance. Government investigators may also seek PHR records for those seeking a security clearance. An employer may want the records for a post-hiring review of health.

Depending on the configuration of the PHR and how it interacts with any associated web sites and other resources, the PHR and associated records may also reveal information beyond what is found in a standard health record. For example, suppose that a consumer's daughter has spina bifida. The consumer's health record maintained by his physician may not reveal that information. But the PHR record or profile may. If the consumer constantly seeks information about spina bifida on web sites associated with the commercial PHR company in some way, the record of PHR usage may reflect the consumer's interests through a search history, through participation in a discussion group, or from tracking of ads clicked upon by the consumer. There is a high variability of how these kinds of systems can be set up, and there is a equally high variability in how non-HIPAA covered PHR systems may approach privacy controls.

PHRs and Privacy Policies

For a non-HIPAA covered PHR, the privacy policy becomes a key document, if it is available. The privacy policy of a PHR vendor may tell consumers how the vendor plans to use personal information. It is possible that a commercial or advertising-supported PHR will do a good job of protecting its clients from uninformed or casual disclosures of personal or health information. It is also possible that a cautious client will not be able to evaluate a PHR vendor's policy or practice.

Privacy policies and terms of service may, if read carefully, reveal something about the bona fides of the PHR vendor. Here are a few questions to consider.

- Does the PHR vendor disclaim all liability for the availability or accuracy of information?

• Does the policy say that the user must pay the PHR's expenses in case of a lawsuit arising from use of the service?

• Is a user's ability to recover damages limited or excluded in case of harm?

• Does the PHR collect personal information about consumers from other sources (e.g., data brokers)?

• Does the PHR say that it has no control over the use of personal third-party advertising networks?

• Are a consumer's searches stored over time so that the PHR vendor has a search use profile that can be used or shared?

• Does the website reveal when someone else paid the PHR vendor to display information? Are paid links identified?

• What happens to personal information if a user stops using the service?

• Is the user's information completely deleted upon request?

• Can the PHR vendor transfer identifiable information to another country where there are no privacy or security protections?

• Can the vendor transfer information to another company without express permission?

• How many separate privacy policies and terms of service apply to the PHR vendor, and how do they overlap?

• How long are these policies?

• Are the policies comprehensible to anyone other than a lawyer?

• Does the PHR vendor clearly state its relationship to HIPAA? If so, does the vendor say that it is "**covered under HIPAA**"? That statement is much more meaningful than if the PHR vendor says that it is "**compliant with HIPAA**." The term *HIPAA-compliant* is sometimes used by PHR companies that are not covered by HIPAA. This term can be confusing to consumers who do not clearly understand the difference between *HIPAA-covered* and *HIPAA compliant*.

One thing likely to appear in every PHR vendor's privacy policy is the vendor's right to change the policy. PHR vendors are likely to reserve the right to change the policy at any time, without notice, and without the user's ability to object. What that means is that even if a PHR vendor has a current set of policies that protect privacy, the vendor can change those policies at will and

with retroactive effect on previously collected information. If a PHR vendor finds that it is not making a profit, it can amend its rules about sharing information with marketers and try to increase its revenues. It is unlikely that PHR users will have the right to consent before a commercial PHR system changes its privacy policy. As the PHR industry consolidates, there could be a race to the bottom because the vendors who share information more broadly have the best chance to survive.

Conclusion

PHRs that operate outside of HIPAA can negatively affect the privacy interests of consumers in various ways. The best to hope for is that a PHR will not make privacy significantly worse. However, it is not likely that even that weak standard can be met. The existence of electronically available and centralized health information outside the traditional health care system will attract new users and create new risks. The mere adding of health records to a PHR vendor's files may undermine existing privacy protections of old records. Security is a concern for any electronic records. A consumer's ability to control the disclosure of PHR records can easily be compromised. The consumer's ability to correct errors in PHR records may be problematic. Advertising support may not meet a PHR's profit goals unless at least some consumer information is available for close targeting of ads. Promised PHR privacy protections may vanish overnight if the privacy policy is changed.

While PHRs may have some laudable goals, they also are a tempting target for companies or others that want to evade whatever privacy protections remain in the health care system in order to make a profit. Whether the benefits of PHRs are sufficient to overcome the real dangers to privacy remains to be seen. It is something that each potential user of a PHR must consider before enrolling. Any consumer worried about the privacy of personal health information should proceed with great caution before agreeing to sign up for a PHR, particularly those operating outside of HIPAA.

Credits

Author

Robert Gellman

Robert Gellman is a privacy and information policy consultant based in Washington, D.C. http://www.bobgellman.com. Mr. Gellman prepared this report for the World Privacy Forum.

Publication History

Original publication February 20, 2008 at http://www.worldprivacyforum.org. Document URL: http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf