WORLD **PRIVACY** FORUM

World Privacy Forum Consumer Advisory:

The Potential Privacy Risks in Personal Health Records Every Consumer Needs to Know About

February 20, 2008

Personal Health Records – or PHRs – are a new trend in health care. 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. PHRs are often touted as a tool for consumer empowerment. But the privacy risks of PHRs have not been widely discussed. **Consumers need to know that not all PHRs protect privacy in the same way, and some PHR systems can undermine consumer privacy in serious ways that consumers may not be expecting.**

In PHRs, important information about privacy procedures and policies is contained in the fine print, and the fine print really matters. That's because some PHRs are covered under HIPAA privacy protections, but many PHRs are not covered under HIPAA privacy protections. **Few consumers understand that their health care files are not always protected under HIPAA when their files are in a PHR.**

Even PHRs that **are** covered under HIPAA can present potential privacy issues. However, HIPAA does provide some baseline privacy protections.

Here is additional information about PHRs and privacy.

Not all PHR records are private in the same way as other health information

Not all PHRs have the same levels of privacy protection. Some PHRs are covered under the federal privacy rule known as HIPAA, but many are not. HIPAA stands for the *Health Insurance Portability and Accountability Act*. It is a federal rule that establishes a baseline for health

privacy in the United States. The HIPAA rules establish minimum privacy and security standards for *covered entities*. A *covered entity* is a health care provider, health insurer, or clearinghouse.

Records in PHRs that are covered under HIPAA have built-in standards for privacy and security, including standards governing disclosure, access, correction, and other privacy elements. Many experts believe HIPAA's protections are weak. It is true that HIPAA is not a privacy cure-all. But even the weak HIPAA standards still supply some protections.

Don't assume your medical records are protected no matter where they are: HIPAA privacy protections generally do not follow the health care files

HIPAA's protections generally do not "travel" with or follow a medical record that is disclosed to a third party outside the health care treatment and payment system. If a health care provider (such as a hospital or a pharmacy, etc.) or a health plan maintains a health care record, the record is protected under HIPAA. But if a third party that is not a *covered entity* under HIPAA obtains the records, then HIPAA does not usually apply.

Look before you share: the details are in the fine print

A good way to discover if a PHR is covered under HIPAA is to find the written privacy policy for the PHR. It is important to read the privacy policy of all PHRs, as well as the terms of use, if available. The PHR's privacy policy should disclose clearly if the PHR provider is a covered entity under HIPAA or not. The PHR's privacy policy should also reveal any disclosures or secondary uses of PHR information that will made, if any.

PHR privacy policies may contain key phrases that can sometimes give you clues about whether a PHR is covered under HIPAA or not.

- Look for the phrase ***HIPAA covered,*** or ***HIPAA-covered entity.***

  HIPAA covered or ***covered under HIPAA*** or ***HIPAA-covered entity*** are phrases a health care provider or health plan may use when describing a sponsored PHR. This phrase usually means that the PHR is covered under HIPAA.

- Don't be misled by the phrase ***HIPAA compliant*** or ***compliant with HIPAA***.

  Sometimes companies offering PHRs that are **no**t officially protected by HIPAA may write in a privacy policy that the PHR is ***HIPAA compliant.*** The phrase ***HIPAA compliant*** can be misleading because it does not always mean that the PHR is actually covered under HIPAA.

If you have any doubts or questions about whether or not a PHR you are considering using is a covered entity under HIPAA or not, ask the sponsor if the PHR is a covered entity under HIPAA.

If the PHR is not covered by HIPAA, the health information may be handled in ways you do not expect

After you have disclosed your health care information to a PHR outside the privacy protections of the health care system (HIPAA), your information can be used or redisclosed by the PHR in ways that would not be permitted for the same information if held by your doctor or health plan.

Depending on the applicable privacy policy, health records outside of HIPAA can potentially be bought and sold, shared with merchants, and even disclosed to employers.

Records outside of HIPAA may also lose certain legal protections. For example, the HIPAA protections covering subpoenas of health records will not apply to PHRs (unless a covered entity operates the PHR). A non-HIPAA covered PHR company could potentially establish a privacy policy that requires it to give its customers, for example, notice of a subpoena, but a privacy policy can be changed at any time. For more details on this topic, see the World Privacy Forum's legal and policy analysis of this issue: *Personal Health Records: Why Many PHRs Threaten Privacy*, available at http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf.

It is crucial to pay attention to what consent forms you are signing or checking off in any PHR

Pay close attention to how all PHR vendors obtain consent, and for what purpose. You may be asked to consent at varying times when you use a PHR. How this happens will vary widely depending on the PHR system.

Pay close attention to the registration pages. These pages may include check boxes that, if checked, will allow greater use and sharing of your data. Sometimes, check boxes are pre-checked and are located in out of the way places, for example, at the bottom of a page. Just signing up to for a PHR may constitute consent for some disclosures of your information.

If you decide to allow greater use or sharing of your information, find out what specific data will be shared, and how you can control that sharing. Remember that once you allow your information to go to a third party, any privacy protections may disappear. That third party may be able to use your data without restriction, depending on the applicable policies.

Read all PHR privacy policies very carefully to find out how consent works at the PHR, and find out how you can withdraw your consent if you decide to later on. See if it is possible to withdraw your entire record from the PHR so that no traces remain.

All PHRs are likely to make some disclosures of information

If the PHR **is** covered under HIPAA, covered entities may still disclose your files without your consent under some circumstances. These circumstances are determined by HIPAA, and may be strengthened by some state laws. The rules for files in PHRs will not usually be very different from the rules that already apply to your health care records.

If the PHR **is not** covered under HIPAA, the disclosures and consents are usually listed in a privacy policy or terms of use. The disclosures of a PHR not covered under HIPAA may be quite different from what HIPAA allows. In a non-HIPAA covered PHR, you may potentially be consenting to more than you realize, especially if you did not read the fine print. A general consent may allow the PHR company to use and disclose personal information for marketing, to track your activities on its website, and to share your data with advertisers.. It will depend on the company's privacy policies, and there can be high variability between PHR policies.

Reading the fine print of advertising-supported PHRs is essential

Some PHRs are supported by advertisements directed to users of the PHR system. In any ad-supported PHR, read the fine print before you click on an ad. Unintended disclosures of health information can pose risks. The privacy policy of an ad-supported PHR should give details about how information is shared with advertisers, what kinds of information about you an advertiser receives, how the advertiser can use that information, and for how long. Ad-supported PHR systems can have substantial differences in how they share information with advertisers and what kinds of controls they put on the advertisers.

In some cases, PHRs may also have tools like specialized search engines, articles on health conditions, and discussion groups as part of their PHR product offerings. Be aware of the policies regarding what happens to the search terms you type in and how your browsing history and other activities are handled. If, for example, you search for a rare genetically-based disease while at a PHR provider's search engine, then read a series of articles there about the same disease, order a genetic test online from an advertiser, and then store the results of the test in your PHR, those activities can say a lot about you by inference. All of that information about your searching, testing, and test results may vulnerable to use and disclosure by the PHR.

Make sure that all of your activities at PHRs are as private as you want them to be. Check and re-check the fine print. If the fine print doesn't tell you everything you need to know and establish policies that protect your privacy, take your business and your records elsewhere.

When accessing any PHR, practice good computer hygiene

Beyond the question of whether or not a PHR is covered under HIPAA, it is important to observe sound computer hygiene when utilizing or accessing a digital PHR. Be sure you are using good firewall, virus, and spyware protection. Ensure that you don't have any software programs running that will capture your online browsing activities and archive data for later retrieval. Some PHR systems use end-to-end, high-level encryption as a security measure, which is something you should look for. (Often, this is disclosed in the security section of a privacy policy. If not, ask the PHR provider about what kind of encryption, if any, is in place.)

Avoid accessing your health care information online from computers at your place of employment or in a public computer terminal with multiple users, such as at a public library. If the PHR displays online ads in the PHR itself or on nearby pages, be very aware of what information is flowing to the advertiser before you click on an ad or offer. Don't click if you don't know the details.

Alternatives to third party PHRs

If you are nervous about giving your health information to a PHR provider, one alternative is to maintain your own records. You have the right to obtain a copy of your health records from your health care providers and health insurers, and this is something that is generally a good idea. There are software tools that you can use on your own computer to help keep your records organized, or if you wish, you can store your files in other formats, such as paper or on discs. The American Health Information Management Association has a helpful and useful site on this topic, http://www.myphr.org/.

For more detailed information about privacy and PHRs, see *Personal Health Records: Why Many PHRs Threaten Privacy*, available at http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf.

Publication history

First publication:
February 20, 2008 at http://www.worldprivacyforum.org.

Document URL:
http:www/worldprivacyforum.org/pdf/WPF_PHRConsumerAdvisory_02_20_2008fs.pdf.

Authors:
Robert Gellman and Pam Dixon.