

# COMPUTERWORLD

## Security

### Privacy group sounds alarms over personal health records systems

Jaikumar Vijayan

**February 20, 2008** (Computerworld) In some cases, people whose health care information is stored in online personal health records (PHR) systems may be exposed to serious data privacy risks, according to a warning issued by a privacy advocacy group.

That's because not all PHR systems are covered by the federal Health Insurance Portability and Accountability Act, the World Privacy Forum said in a 16-page report released today ([download PDF](#)). The WPF contended that as a result, many of the privacy protections offered under the HIPAA statute don't apply to the personal health care data being maintained in such systems.

PHR systems typically store medical records gathered from a variety of sources, including health care providers, insurers and patients themselves. The information is made accessible via the Web to individuals and to others who they have authorized to view the data. "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," the San Diego-based WPF noted in its report.

But people need to be aware that the systems may fall outside of HIPAA's protective umbrella, said Pam Dixon, the group's executive director. The HIPAA privacy rules cover health plans, doctors, hospitals, clinics, nursing homes and even researchers working with medical data collected from those entities, she said. But commercial PHR systems maintained by IT vendors or services providers and supported by means such as advertising may not come under HIPAA's purview, according to Dixon.

And even in cases in which a PHR system is covered by HIPAA, there are circumstances under which an individual's medical records may not be protected, Dixon said. For instance, she pointed to medical information that a person puts into the PHR system on his or her own behalf.

There are several problems that could result from the lack of privacy protections, Dixon said. For starters, she claimed, health records could lose their privileged status if a patient authorizes a doctor to send a copy of the information to a PHR system that isn't covered by the HIPAA mandates.

"Many consumers have this deeply held belief that their health information, no matter where it travels, is protected in the same way as when you have a doctor/patient relationship," Dixon said. In reality, consenting to have data transmitted to a noncovered system likely would be viewed as an indication that you had waived your privacy privilege, she added.

Health information stored in commercial PHR systems is also less protected against subpoenas than it otherwise would be, Dixon asserted. Under HIPAA, if someone seeks to subpoena medical records about an individual from a covered entity, the patient has to be informed first. But that protection doesn't apply to PHRs in all instances, she said.

"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 WPF noted in its report. "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."

Even more worrisome to Dixon, though, is the potential for protected medical information stored in PHRs to be used for marketing purposes. HIPAA explicitly prohibits such uses, but the terms under which many PHR systems are operated could enable their owners to sell personal health data to marketers, she said.

People should be aware of such issues when choosing whether to use PHR systems, Dixon said. She added that the operators of PHR systems should be required to clearly disclose whether they are covered under HIPAA and what sort of privacy protections they offer.

The WPF's report raises some important, if long-standing, issues, said Peter MacKoul, president of HIPAA Solutions LC, a Sugar Land, Texas-based firm that offers a set of tools and services to help companies comply with HIPAA. "We see some serious privacy violations" within PHR environments, MacKoul said.

But he added that a bill proposed in the U.S. Senate last summer by Sen. Patrick Leahy (D-Vt.) should address the issues cited by the WPF if it is passed by Congress and signed into law. The bill, called the Health Information Privacy and Security Act and referred to by the number [S.1814](#), would provide individuals with access to their health records and ensure personal privacy with respect to that information, MacKoul said. One of the bill's provisions, he noted, touches on the issue of health-information data brokers and their privacy responsibilities.

The bill was referred to the Senate Committee on Health, Education, Labor and Pensions after it was introduced by Leahy. No further action has been taken thus far, according to information posted on the Senate's Web site.