Overview:
Best Practices for Employers Offering
Personal Health Records (PHRs)

December 2007

PHRs, Employers, and Privacy

Over the past year a group of leading companies has joined forces to address hurdles to offering Personal Health Records (PHRs) to their employees. Convened by the California Healthcare Foundation and IBM, the group agrees that PHRs hold the promise to improve healthcare, lower costs, and give people the tools to better manage their own health, but that privacy risks and other consumer concerns must be addressed upfront. A number of employers are already offering PHRs in some form, while others are at earlier stages of development.

Healthcare should benefit from the same increase in consumer access to information that is transforming the banking and travel industries. But, of course, healthcare is different, in part because of the extreme sensitivity of health information, and in part because of the complexity of healthcare itself. Once misused, lost, or stolen, health information, unlike dollars, can never be returned—the damage is done.

And in fact, the public's fears about health privacy are linked in part to employment, as documented by a 2005 California HealthCare Foundation survey in which more than half of participants voiced concerns about employers potentially using health information to limit job opportunities.[1] Further, a recent survey by the National Business Group on health found that a vast majority of employees, if offered a PHR by their employers, would want to decide what information it contained and who had access to that information. Most strikingly, 85% said it was "important" or "extremely important" that their privacy be protected and that their employer be prohibited from accessing the PHR.[2]

[1] See the California HealthCare Foundation's "National Health Consumer Privacy Survey 2005" at http://www.chcf.org/documents/ihealth/ConsumerPrivacy2005ExecSum.pdf

[2] http://www.ihealthbeat.org/articles/2007/12/7/Survey-Employees-Tap-Internet-for-Additional-Health-Information.aspx

The Employers' Working Group on PHRs
In addition to several Fortune 500 companies and other leading corporations, the *Employers' Working Group on Personal Health Records (PHRs)* includes information technology and policy experts from foundations and non-profits, including the Center for Democracy and technology (CDT), the Health Privacy Project, which staffs the effort, and The Markle Foundation. Representatives from several companies that currently offer PHR products (or plan to in the near future), such as WebMD, Google, and Revolution Health, also participate.

The "Best Practices" developed by the group are intended to serve as guidance for employers offering PHRs in developing and refining privacy policies and practices, notices to employees, and education and training activities. *The Employers' Working Group* plans to expand its membership, and to develop a Model Notice to further implementation of the Best Practices. The goal is to develop aspirational guidelines—not a one size fits all solution—taking into account varying state and federal laws, and a range of business practices, in an effort to achieve more substantial uniformity in employer practices and consumer expectations and trust. The Working Group agrees that these concerns must be addressed if PHRs are to succeed in improving healthcare quality.

Studies released by Kaiser Permanente (May 2007)[3] and California HealthCare Foundation (CHCF) (November 2005)[4] document that the public believes that a paper-based medical records system is more secure than a computer-based one. Numerous recent breaches of digital health and other types of data (for example, from a US Department of Veterans Affairs laptop) add to consumer anxiety about electronic health information. The CHCF survey and one released by Mathematica (April 2007)[5] document that racial and ethnic minorities, and people with chronic illnesses, mistrust the security of electronic health records systems, and are more likely than whites to withdraw from full participation in their own care to avoid potential stigma and discrimination by employers and others.

Nevertheless, reports by the Markle Foundation[6] and Forrester Research[7] document a strong public desire for PHR services. And the recent survey by the National Business Group on Health indicates that the Best Practices are on the right track in encouraging employers to establish consumer control and trust in a PHR context. As referenced above,

---

[3] "Health Care Information Technology Survey Results," May 2007 by Kaiser Permanente, http://xnet.kp.org/newscenter/kphealthconnect/2007-07-09-b.html
[4] "National Health Consumer Privacy Survey 2005," by the California HealthCare Foundation, http://www.chcf.org/documents/ihealth/ConsumerPrivacy2005ExecSum.pdf
[5] "Considerations in Designing Personal Health Records for Underserved Populations" by Ann Bagchi, Lorenzo Moreno, and Raquel af Ursin, April 2007, Mathematica, http://www.mathematica-mpr.com/publications/pdfs/hlthcaredisparib1.pdf
[6] "Americans See Access to Their Medical Information As a Way to Improve Quality, Reduce Health Care Costs," 2006 by the Markle Foundation. http://www.markle.org/resources/press_center/press_releases/2006/press_release_12062006.php
[7] See for example "Are Personal Health Records Breaking Out?" by Lynne Sam Bishop, June 2006, Forrester. http://www.forrester.com/Research/Document/Excerpt/0,7211,39415,00.html

a vast majority of employees, if offered a PHR by their employers, would want to decide what information it contained and who had access to that information. In addition, 85% said it was "important" or "extremely important" that their privacy be protected and that their employer be prohibited from accessing the PHR. The Best Practices give employers a significant tool to use in fostering consumer trust and confidence, and addressing existing concerns with meaningful policies and practices.

Overview of the Best Practices

The text of the ten Best Practices is followed by a short note on the Practice's importance, and implementation tips.

1. Transparency and Notice

> Employers should be transparent about their reasons for offering a PHR to employees and all policies that apply to the PHR. Employers should provide an Information Policy Statement or Notice that clearly lays out the ways in which information in the PHR will be used and safeguarded. Employers should incorporate the Notice into their health benefit programs, and should make it available in a layered format—a short concise version to accompany a more detailed one. Employees should be informed of any updates to the policy.

Transparency is fundamental to the success of an employer-sponsored PHR because it helps to establish trust. A Notice or Information Policy Statement about the PHR is one of the best manifestations of transparency—it should be accessible to and understandable by employees. The Best Practices are designed to give employers direction as they develop the policies and practices that apply to a PHR. To assist employers in development of a Notice, the Working Group is currently writing a Model Notice that includes sample language in addition to a list of questions and considerations employers should address. The Model Notice will be released in 2008.

2. Education

> Employees should be educated about the benefits, functions, and content of the PHR. Information about the PHR should be communicated in numerous ways to build both knowledge and trust.

Sound and transparent policies concerning PHRs will be valuable only if employees are aware of them. Educational content may be conveyed via a benefits package at the time of enrollment, group meetings, or a memo from the CEO, among other options. Information must be accessible in a variety of languages and formats depending on the needs of the employee population.

3. Employees Can Choose which Content is Included in the PHR

Employees should be able to determine the content of the PHR, including which providers and plans contribute to it. Employees should be able to annotate the records submitted by others, as well as to enter their own information, with employee-entered data marked as such. The identification of sources of all personal health information in the PHR should be readily apparent.

Findings of a survey released in December of 2007 by the National Business Group on Health show that a vast majority of employees, if offered a PHR by their employers, would want to decide what information it contained and who had access to that information. Giving employees the latitude to shape the content of the PHR, however, may create concerns about the medical accuracy of the information. This Best Practice recommends identifying the sources of all personal data in the PHR to help employees and others with whom they may share a PHR to decide which information to rely on and to track down the original source if necessary.

4. Employees Control Access to and Use of the PHR

a.) Employees should control who is allowed to access their PHRs. Employers should not access or use employees' individually-identifiable health information from the PHR.
b.) Employees should choose, without condition, whether to grant access to personal health information within their PHRs for any "secondary uses". An audit trail that shows who has accessed the PHR should be easily available to employees.

According to the December 2007 survey by the National Business Group on Health, 85% of employees believe it is "important" or "extremely important" that their privacy be protected and that their employer be prohibited from accessing the PHR. While some members of the Working Group pointed out situations in which it could be beneficial for employers to access individually-identifiable health information from the PHR, the group decided that public concerns dictated that they refrain from doing so in order to maintain trust.

"Secondary uses" are any uses of health information from the PHR that are not directly related to an employee's own clinical care or wellness management. Examples of secondary uses include (but are not limited to) medical research, public health, law enforcement, and marketing.

5. Employees Can Designate Proxies to Act on their Behalf

Employees should determine who, including family members and caregivers, should have direct access to their PHRs on their behalf. Where possible, employees should be able to grant proxy access to full or partial information in their PHRs, including access in emergency circumstances. Employees should also have the ability to revoke access privileges.

The healthcare of an individual often involves collaboration and support from others such as a spouse, parent, child, or other family member, in addition to the input of doctors, nurses, and home health aids. Regardless of the makeup of an employee's health team, it should be possible for him or her to share access to the PHR with others while maintaining a level of control.

6. "Chain of Trust": Information Policies Extend to Business Partners

The information policies and practices of employer-sponsored PHRs should follow the data through chain of trust agreements that require business partners to adhere to the employer's applicable policies and practices.

An employer's sound business policies concerning a PHR--and thus the employee trust that depends on them—can be undermined if data is handled poorly by business partners who have access to it. A business partner is any third party entity with which the employer has a contract or business relationship that pertains to the PHR or the information in it. Examples of business partners include disease management companies and companies that provide PHR services on behalf of the employer. Being bound by a "chain of trust" means business partners must adhere to the policies put forward by the employer in its Information Policy Statement.

7. Data Security

Employers should provide a strong level of security to safeguard the information in the PHR systems. A robust authentication process for access to PHRs should be required, in addition to an audit trail that shows who has accessed information and when.

The need for this Best Practice and the following one should be fairly evident; employers should help employees to understand their particular security measures and, in the event of a breach, make information from the audit trail available to them.

8. Data Management

Employers should ensure that the PHR systems they provide have comprehensive data management strategies that protect the integrity of the data and include data retention policies.

Strategies to protect data integrity and provide retention could be very important to employees, particularly in the case of unexpected events such as natural disasters.

9. Enforcement and Remedies

Employers should establish oversight and accountability mechanisms for adhering to their PHR policies and practices. Employers should put into place a mechanism to promptly notify employees of any inappropriate access to or use of information contained in an employee's PHR, identify the steps which have been taken to address the inappropriate activity, and make resources available to employees to assist them in addressing the effects of the inappropriate activity.

No matter how comprehensive an employer's PHR policies and practices may be, unexpected errors may occur. An essential element of maintaining employee trust is establishing (ahead of time!) an open and honest process for responding to them.

10. Portability

Employers should offer PHRs that are portable, to the extent feasible, allowing employees to maintain or move the PHR and/or the data it contains even after employment or coverage ends or changes.

PHRs are meant to be tools for employees. As such they should be available to employees for long-term use, regardless of their employment status.

The *Employers' Working Group on PHRs* is convened by the California HealthCare Foundation and IBM. The Health Privacy Project and Clear Voice Consulting provide staffing for this initiative. For more information, see www.healthprivacyproject.org/bestpractices.