HEALTH
PRIVACY
PROJECT

Best Practices for Employers Offering Personal Health Records (PHRs)

December 2007

Developed by the Employers' Working Group on Personal Health Records (PHRs)*

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

* Members of the *Employers' Working Group on PHRs* include representatives from the following companies and organizations:

> **Center for Democracy & Technology, Dell, Google, Hewitt Associates, IBM, Markle Foundation, Omnimedix Institute, Pfizer, Pitney Bowes, Revolution Health, Wal-Mart, and WebMD.**

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, including a background paper on the Best Practices, see www.healthprivacyproject.org/bestpractices.

GLOSSARY

Business Partner – A business partner is any third party entity with which the employer offering a PHR to employees 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. Business partners must be bound by a "chain of trust" – in other words, they must adhere to the policies put forward by the employer in its Information Policy Statement.

Individually-Identifiable Health Information
Individually-identifiable health information is traceable to a particular person. By contrast, non-identifiable aggregate information refers to a compilation of anonymous data about many people. However, given the lack of widely-accepted guidelines defining "individually-identifiable" and "non-identifiable," it is advisable to be cautious. While a single piece of information (such as a birth date) may not alone be enough to identify a particular person, the addition of other data about the same person, such as name, zip code, place of work, etc. makes it easier to verify his or her identity. As the total volume of data collected grows and increasingly sophisticated tools for analyzing it become available, it becomes easier to identify the source of almost any information.

Information Policy Statement – An information policy statement (or "notice") is a statement by a company or organization that describes how it handles information. The information policy describes procedures that relate to the protection of privacy and other rights and responsibilities of the organization and other entities (including the employee) with which it interacts.

Personal Health Information – Personal health information includes any information pertaining to an individual's health. The term encompasses clinical information (for example, a list of medications a person is taking) and also behavioral or other non-clinical information (for example, a description of an exercise or diet regime). Originators of personal health information include but are not limited to healthcare providers, labs, and the individual consumer or patient. Personal health information may or may not be traceable to a particular individual (see also "individually-identifiable health information").

Personal Health Record (PHR) – The PHR is a tool that contains digital health information about an individual for his or her own use. A PHR may be used to compile various information, such as basic health data (e.g. height, blood type), a record of illnesses and injuries, prescribed medications and other treatments, test results, allergies, and the health histories of family members. While the PHR is distinct from a physician's medical record, it is likely to contain copies of much of the same information. The PHR may serve as a repository of information that originated from different sources, including general practitioners, medical specialists, labs, and pharmacies—in addition to information input directly by the individual. It may also include a variety of tools and services to help individuals to manage their own health.

Secondary Uses – 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, and marketing.

Third Party – A third party is any entity not directly involved in the provision of PHR services which may potentially have access to the information from a PHR. Examples of third parties include business partners of the employer, public health agencies, health research organizations, law enforcement agencies, and courts of law.