

March 31, 2009

Health Information Security and Privacy Collaboration

Personal Health Record (PHR) Website Inventory, Analyses, and Findings

Prepared for

RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Policy Analyst
Office of Policy and Research
Office of the National Coordinator for Health IT
200 Independence Avenue, SW, Suite 729D
Washington, DC 20201

Prepared by

Consumer Education and Engagement Collaborative
Massachusetts



Contract Number HHSP 233-200804100EC
RTI Project Number 0211557.000.007.100

Contract Number HHSP 233-200804100EC
RTI Project Number 0211557.000.007.100

March 31, 2009

Health Information Security and Privacy Collaboration

Personal Health Record (PHR) Website Inventory, Analyses, and Findings

Prepared for

RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Policy Analyst
Office of Policy and Research
Office of the National Coordinator for Health IT
200 Independence Avenue, SW, Suite 729D
Washington, DC 20201

Prepared by

Jerilyn W. Heinold, Massachusetts
Diane Stone, Massachusetts
Marisa MacClary, Massachusetts

Identifiable information in this report or presentation is protected by federal law, section 924(c) of the Public Health Service Act, 42 USC. § 299c-3(c). Any confidential identifiable information in this report or presentation that is knowingly disclosed is disclosed solely for the purpose for which it was provided.

Contents

Section	Page
1. Introduction	1
2. PHR Inventory	1
2.1 Methods	1
2.2 Framework for Analysis	1
2.2.1 What Is the PHR Offering?	2
2.2.2 What Critical Information Do I Need to Know About the PHR Services As Described on Their Website?.....	2
2.2.3 What Are My Health Care Needs?.....	2
2.2.4 How Do I Match Their Offerings to My Health Care Needs (the decision to purchase)?.....	2
2.3 Findings	3
2.3.1 Company Affiliation	3
2.3.2 Product Description	3
2.3.3 Media Used	4
2.3.4 Data Origin and Input.....	5
2.3.5 Audience for PHR Information Collection	5
2.3.6 Privacy and Security.....	6
2.3.7 Secondary Uses of PHI	7
2.3.8 Cost	8
3. Conclusion	1
Appendix A Inventory Matrix for Personal Health Records	

Figures

Number	Page
2-1. A Visualization of Consumer Decision Making for PHR Choice	2-2

Preface

This report presents an analysis of publicly available personal health record (PHR) services: who sponsors them, what information is included, and how they treat categories of sensitive health information. It also provides background information that organizations can use to educate and engage consumers about how PHRs address privacy and security issues and sensitive health information.

1. INTRODUCTION

The personal health record (PHR) has been defined as “an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.”¹ However, not all products or services marketed as PHRs meet this definition. For example, some PHR products or services may use information in PHRs for secondary uses that are outside an individual’s control.

Nonetheless, PHRs are emerging as a way to aggregate and store one’s health information, and many types of products and services marketed as PHRs are reviewed in this report. Currently, PHR characteristics are extremely diverse including, for example, the types of health information collected, the way health information is entered, the ability to import and integrate physician and hospital information, and the way each entity protects sensitive information (privacy and security attributes).

The purpose of this project was twofold:

- To create an inventory of the characteristics for selected PHRs, including standalone, tethered, and aggregated versions, with specific attention to sensitive information and privacy and security concerns.
- To develop a plain language consumer guide to help consumers understand PHRs, including their purpose, value, range of services, terminology and definitions, and importantly, how to use this information to evaluate current choices in products marketed as PHRs.

¹ National Alliance for Health Information Technology. (2008). Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms. Retrieved January 29, 2009 from http://www.nahit.org/images/pdfs/HITTermsFinalReport_051508.pdf.

2. PHR INVENTORY

2.1 Methods

We searched the American Health Information Management Association (AHIMA) website <http://www.myphr.com> to select PHR websites to include in this analysis. After excluding websites that were inaccessible or were not PHRs, we selected 92 websites from 109 listed on the AHIMA website to include in our analysis. We developed initial categories for the inventory information collection, which included:

- product name and URL,
- format for data entry, product description,
- data origin,
- privacy and security statements (access and control),
- handling of sensitive information,
- audience/target population,
- cost, and
- “of note” (positive points and concerns).

As we reviewed and analyzed each website, we added the following categories and subcategories to provide a broader baseline for consumers to consider: type of media used, company affiliation and mission, specific data the PHR collects, secondary use activities, usability, and availability of demos. Demonstrations of the various programs were not accessed or evaluated for this study. A more detailed description of the categories and findings follows. Data were entered into a MS Excel inventory matrix (see **Appendix A**), and all data were checked for consistency. Random checks were performed to confirm accuracy.

2.2 Framework for Analysis

A consumer-centric framework was constructed to better understand the information that would best help a consumer choose among various PHRs. It began with a hypothetical consumer perspective, summarized as:

“I have decided that I need/want a place for my health information including sensitive information. How do I decide on a safe choice (where safe means a good comfort level regarding: access control, security risks, and safeguards)?”

This approach assumed that the consumer, using a web-enabled computer, was preparing to make a decision to sign up, join, or purchase a PHR product or service. **Figure 1** displays

a model for PHR choice. Once the consumer accesses a PHR website, he/she must determine the answers to the questions in the following sections.

2.2.1 What Is the PHR Offering?

Offerings could include personal information, the mode of data entry, the data collected, and the services available, including, for example: care management, summary for emergency/travel, case management, disease management, alerts, trends, information to discuss with provider, coaching, health community, advanced directives, and new products. Information could be stored on a device or be web-based.

2.2.2 What Critical Information Do I Need to Know About the PHR Services As Described on Their Website?

Critical information could include privacy and security safeguards, handling of sensitive information, ease of use, available demonstration, and company affiliation/mission.

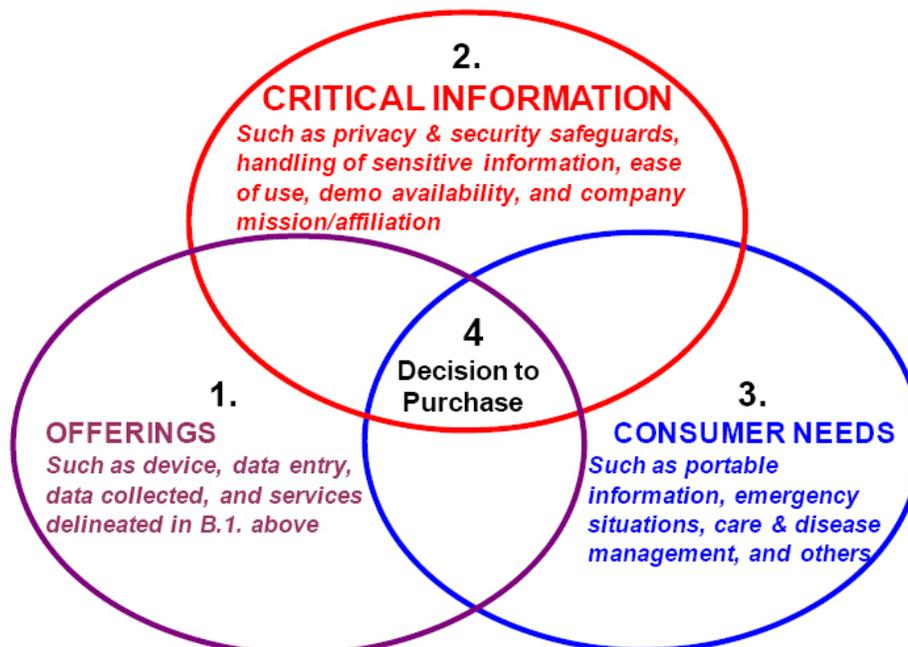
2.2.3 What Are My Health Care Needs?

Health care needs could include portable information, conversations with my provider, emergent situations, preventive care, care/disease management, and extra help such as advocacy, coaches, and clinical decision support.

2.2.4 How Do I Match Their Offerings to My Health Care Needs (the decision to purchase)?

Figure 2-1. A Visualization of Consumer Decision Making for PHR Choice

(The labels 1, 2, 3, 4 correspond to the sections above.)



2.3 Findings

We collected information from PHR product and service websites using the categories listed in the following sections. We selected these categories to facilitate the consumer's decision-making process (as described in the previous section). This section provides greater definition of and rationale for the categories we chose.

2.3.1 Company Affiliation

Knowing a PHR's company affiliation can serve as a good indicator of the purpose and mission that drive the comprehensiveness for PHR information collection and access. Affiliation also may identify the business model or purpose for the PHR service. Most PHR services are U.S.-based.

Based on a review of websites, we found that PHR products and services range from "humanitarian" through "for-profit business expansion."

1. **Humanitarian:** a single person recognizes the need, based on a first-hand medical situation, and develops a PHR product or service so that others do not face the same problem, such as the inability to obtain necessary protected health information (PHI) in a medical emergency or course of treatment. Often, a foundation supports this type of PHR service. Fewer than 10% of the reviewed PHR sites were established for humanitarian reasons.
2. **Government:** both the federal government and several state PHR sites were identified, all based on the recognition that it is better to collect this information before access to it is necessary. PHR websites, such as the one offered by the U.S. Department of Veterans Affairs, and three states represented a small percentage of the overall total of websites.
3. **Health care organizations ("covered entities"):** large provider offices or health systems, health plans/insurers, have created PHR websites to assist in the electronic availability and accuracy of patient demographics and medical information. These organizations adhere to the rules for "covered entities" or business associates of covered entities under HIPAA. Fewer than 20% of the reviewed PHR sites were identified as health care organizations.
4. **Core business:** a company that has recognized a population need and developed the PHR product; can be for profit or not for profit. Close to half of the reviewed PHR sites were in this category.
5. **Business expansion:** an existing company that develops a PHR product or service as a mechanism for increased market share and to complete a marketplace offering for comprehensive record keeping. Approximately one quarter of the reviewed PHR sites fell into this category.

2.3.2 Product Description

Types of products or services we identified include:

- Stand-alone PHR: Platform designed to use the data that exist after input by the consumer. They do not consolidate information directly or indirectly from physician

- Tethered, portal-based, aggregated, and integrated: PHR platforms that electronically integrate information across multiple data inputs including ancillary streams. The terminology denoting this attribute is not currently distinctive. Sometimes there is significant overlap in these terms. Thus, a health care portal that is maintained by a health plan may also be tethered, allowing the patient to look at his/her lab values but also allowing the patient to enter additional (for example, diet and exercise data).

2.3.3 Media Used

The product description includes the type of media used; several different types are available for storing and using PHR information. The media type seemed to be evenly divided between stand-alone software and Internet-based repositories. This category is significant because the privacy and security issues associated with each are different. Removable media such as thumb drives, cards, and key chains contain all the personal information or the PHI needed for an emergency. Thus, the individual controls the PHI; however, the risk is that these may be lost or stolen or not kept up to date. In addition, the individual consumer is solely responsible for backup of the data. Other uses of individual PHI, i.e., data mining or resale, are not significant risks for removable media. However, for those products with PHI that reside on a web server, privacy and security concerns are paramount. Many of the PHR sites are strictly business vendors and are not covered entities subject to HIPAA compliance requirements. Consumers need to look at the privacy policies and statements, and security procedures and process descriptions carefully, because not all PHR services ensure confidentiality in the use and disclosure of PHI. (See additional discussion in **Section 2.3.6**, Privacy and Security.)

The reviewed PHRs use the following media for PHI collection:

1. The majority (approximately 60%) of the PHRs were **web-based services** offering a combination of patient-entered, patient-entered and health care entity downloaded data, or a patient-entered and software liaison-entered format.
Approximately 40% of PHR websites offer software that resides on the consumer's computer, including the media categories described below:
2. **Removable drives** including thumb drives and CDs (approximately 10% of the reviewed sites).
3. **Nondigital cards** including paper/cardboard and sometimes created as key chains (approximately 5% of the sites).
4. **Metal bracelets, pendants, watch bands** that have been available as medical alerts for many years (less than 3% of the PHR sites).

2.3.4 Data Origin and Input

The data origin and input category was overwhelmingly dominated by patient-entered data. The majority of products employ data questionnaire screens or electronic interview-driven screens for consumers to enter their information. Exceptions include health plans/insurers, large physician organizations, data platforms such as Microsoft HealthVault and GoogleHealth, and some employers who offer patient portals as a way for employees to access their health care information. Patient-entered data has the potential to be problematic for many reasons, including the variation in completeness based on memory and an individual's reluctance to spend the time and effort completing the PHR questions and sections. The consumer would also be responsible for keeping the information up-to-date and accurate; a task that is now accomplished, for the most part, by physicians or other caregivers as part of an electronic medical record (EMR) or electronic health record (EHR) system.

2.3.5 Audience for PHR Information Collection

The audience identified types of users who would benefit from the organized and consolidated collection of personal medical information. The review of PHR products and services showed a range of purposes from the simple consumer "owner" user who would benefit in treatment situations from an initial effort to consolidate and maintain PHI, to allied health product companies that can offer care management and support services to the consumer based on stated PHI issues. This audience category identified the following types:

1. **The general population:** patients, families, and caregivers represent the greatest target audience for PHRs. As users, these consumers benefit from a single source of PHI for treatment in emergent situations, for treatment, and payment to enhance/supplement the accuracy of provider visits, medical history, school questionnaires, and nursing home care. More than three quarters of the sites targeted this audience.
2. **First responders:** emergency services and medical staff clinicians who can efficiently gain access to, and be able to act on, critical medical information for treatment. Most PHR sites included this audience as critical users of PHRs.
3. **Care management:** clinically trained staff employed as part of the PHR service—a larger diversified business enterprise, a provider office, or the consumer's health plan. These staff can assist the consumer with the collection and assembly of accurate and complete PHI; they can also review and analyze data to provide certain medical condition support, including wellness programs, and health coaching. Approximately one quarter of the PHR reviewed sites offered this service.
4. **Chronic care case management:** while similar to care management, chronic care case management is a targeted high-incidence, disease management approach to ensure that necessary services are supported to keep patients at a high level of functioning. Approximately 10% of the PHR reviewed sites indicated specific value to this population.
5. **High-risk children's health records:** parents and guardians are finding that high-risk children need immediate access to medical records that would include specific

medical condition PHI that goes beyond the routinely collected treatment and provider information, i.e., immunization, height, weight, medications, allergies. Approximately 15% of the PHR reviewed sites indicated specific value to this population.

6. **Elder care:** seniors and their caregivers gain significant value from up-to-date, easy-to-access PHI. Fewer than 10% of the PHR sites indicated elders as the target market.
7. **Medication history:** these PHR products focus on one of the most critical pieces of information in emergent situations. While medication history is a critical data element for all the PHR information collection, approximately 10% of the sites indicated targeted medication history collection.
8. **Health condition affinity communities:** those patients and families burdened with managing medical conditions that challenge the health care community for successful diagnosis, treatment, and outcomes have found online support groups to chat and share advice, ideas, alternatives for comfort and support. Approximately 5% of the PHR websites reviewed indicated that this type of expanded service was offered.

2.3.6 Privacy and Security

Privacy and security for PHR information collection identifies the type or level of confidentiality assurance, information safeguards, and access controls that are in place on the website and for the services offered by the PHR provider. These processes would be followed in storing and protecting a consumer's PHI. Compliance with privacy protections can vary based on the business. State and federal privacy and security laws and regulations extend protections required of covered entities. Federal HIPAA laws define covered entities as: certain health care providers, health plans/insurers, and health care insurance clearinghouses (enrollment and claims). Some businesses also provide direct services on behalf of covered entities (business associates). Business associates generally have contracts with covered entities that require privacy and security protections. However, businesses and services that operate outside privacy and security compliance regulations are not required to protect consumer PHI from unauthorized access, use, and disclosure for care or noncare purposes. Still, many of these businesses and services state they follow privacy and security guidelines. For the consumer, the regulatory protections for privacy and security are of limited consequence if the PHR containing the PHI is a digital device or on the desktop computer, since such data are not stored by a third party and privacy/security is mainly the consumer's responsibility. However, if copies of the PHI are stored in a central repository where other persons could gain access with or without authorization, the consumer should be aware of how his/her PHI would be protected. The categories of privacy and security protection statements that were found on the PHR websites are:

1. **A HIPAA-compliant PHR product or service:** makes direct reference to its position on protecting PHI either because it is a covered entity required to comply with federal law and regulations to protect the use and disclosure of a consumer's PHI, or for business purposes promises to follow HIPAA regulations to add comfort to

the use of the PHR service. Text to this effect will be highly visible on a website page, in a clearly marked dropdown screen, or found at the bottom of the web page. HIPAA compliance is currently considered the trusted seal of approval. Fewer than half of the reviewed PHR sites clearly indicated HIPAA compliance. If the PHR product or service is not a covered entity, there is always a risk that the company may change its policy regarding HIPAA compliance.

2. **Security industry standards adherence:** PHR companies not required to be HIPAA compliant, but committed to safeguarding the security of PHI, will reference the state-of-the-art security functions that are part of the electronic storage of PHI. Consumer authorization, password access and authentication, encryption of data, firewall software, and so forth are all features to protect consumer PHI. Many of the PHR sites indicated “HONcode” compliance. HONcode is an international certification that is being reported (<http://www.hon.ch/HONcode>, Health on the Net Foundation). Its criteria include:
 - authoritative (indicate the qualifications of the authors);
 - complementarily (information should support, not replace, the doctor-patient relationship);
 - privacy (respect for the privacy and confidentiality of personal data submitted to the site by the visitor);
 - attribution (citation of the source(s) of published information, date and medical and health pages);
 - justifiability (site must back up claims relating to benefits and performance);
 - transparency (accessible presentation, accurate e-mail contact);
 - financial disclosure (identification of funding sources); and
 - advertising policy (clearly distinguishing advertising from editorial content).

More than a quarter of the reviewed PHR sites stated that security industry standards were followed, or that secure portal access was in place.

3. **No reference to protecting data:** approximately a third of the reviewed PHR sites did not mention privacy or security.

2.3.7 Secondary Uses of PHI

Privacy and security considerations for PHR use should include information on the secondary uses of the PHI data that may be intended by the PHR product or service. This term references the intended or nonintended reuse of PHI beyond the initial purpose of PHI collection for the PHR service. Often, reuse is not acceptable from the consumer’s point of view. HIPAA compliant PHRs would have to state their intent to use PHI for secondary uses, and the owner of the PHI would have to actively authorize such a use. Some PHR companies’ business models may actually rely on the resale of PHI to companies that seek to identify consumers for target product or service marketing. Consumers should carefully read the website for a description of the parent company and how it may use their data. This PHR review found the following information regarding secondary uses:

1. **No secondary uses stated:** very few sites fell into this category.
2. **Stated interest in secondary uses, but requires the PHI owner's consent:** approximately 15% of the PHR sites reviewed.
3. **Stated that cookies are used when consumers add PHI**, sometimes just for general maintenance and ease of site use, other times for tagging marketing. Fewer than 20% of PHR sites reviewed fell into this category.
4. **Does not state intent and is silent on privacy protections.** Consumers need to be extremely alert to the potential invasion of privacy. Most of the PHR sites did not discuss secondary uses.

2.3.8 Cost

Cost was noted in the review of sites and, in general, was under \$50; at least 50% of the sites were free or had free trial periods.

3. CONCLUSION

This report has provided background and practical information about PHRs to assist both those involved with this evolving part of electronic health information exchange as well as consumers who can benefit from the basic vision and purpose of centralizing personal health information. The fundamental benefits of PHR products—to reflect a consumer's total health history and to act as a tool for preventive health and care management—are just beginning to be embraced and have not been truly tested or realized. Nonetheless, the rapid evolution of new features and attributes that make PHRs easier for consumers to use and maintain is encouraging. PHRs can be highly valuable tools because of the opportunities they offer to improve safety and quality of care in emergent situations or when tests are ordered, to empower patients to play a more active role in their care, and to help individuals better manage the care of family members or friends who are unable to do it for themselves. They will most likely be part of the redirection of health care towards a more consumer-centric delivery system. However, as PHRs evolve and the marketplace “shakes out” to consolidate with the products and PHR services that align with electronic health information exchange, the following challenges must be addressed:

- lack of clear policies protecting consumers' privacy and security including how sensitive health information should be handled/categorized within PHRs;
- lack of explicit notices regarding consumer control/consent for secondary uses of their PHI;
- widespread integration with provider systems so that consumers can more easily keep their records accurate and up to date;
- ensuring data accuracy and completeness when consumers enter their own data; and
- clear differentiation of PHR product features and attributes so that consumers can easily select the best product for their specific needs.

The certification of PHRs and their associated standards, beginning in summer 2009 by the Certification Commission for Healthcare Information Technology, may be a good start to dealing with some of the inherent privacy and technical issues listed in this report. Other organizations like Connecting for Health's Markle Foundation, the Healthcare Information Technology Standards Panel, and the American Health Information Management Association are contributing to the future design of PHRs so that these products and services become a trusted, effective, and consumer-centered health care solution.