Keeping Online Personal Records Private: Security and Privacy Considerations for Web-based PHR Systems

Save to myBoK

by Anil Srinivasan

As Web-based personal health record (PHR) systems grow in popularity, it is important that they be managed and maintained responsibly. Online PHRs must provide the same security and privacy controls required of other electronic systems that handle personal health information. This article presents key security and privacy considerations and reviews ways to mitigate consumer concerns surrounding Web-based PHR systems.

Growth in Online PHRs

Three trends are converging to connect consumers with their health information online. First, providers are increasingly managing patient health information electronically, which increases its accessibility. Secondly, more providers are seeking ways to allow patients easy access to their information, and they are interacting more with their patients online. Finally, consumers themselves are actively seeking health information on the Web.

Reports have highlighted the advantages of compiling information about lifestyle, health status indicators, risk factors, and personal and family health history. The more patients know about managing their health, and the more providers know about a patient's complete history, the better the patient's health. To this end, the concept of a complete personal health record system has emerged in recent years. The PHR is a way for consumers to collect and share their health histories with providers, and they can serve as a way for providers to share health information such as test results or targeted educational material with consumers.

Early electronic PHRs were based on offline media such as smart cards, CDs, and thumb-drives. In these models, patients carry their information with them and fully control access to it. However, these systems lack standard infrastructure, and they often require proprietary software to read and write information. As a result, the more recent and popular PHR systems are increasingly Web-based.

Web-based systems are typically sponsored by healthcare providers, insurance companies, or commercial third-party vendors. These systems offer the benefit of round-the-clock access from any Web browser. They allow patients to communicate with multiple providers while still controlling and managing access to their information.

Ensuring Consumer Confidence

At a time of seemingly constant reports of online security breaches and theft of sensitive personal information, it is imperative that PHR systems instill consumer confidence. If consumers doubt the security of online PHR systems, they will not adopt them. Handling customer information responsibly is critical to the success of online PHR systems.

Consumers have greater trust in a system where they control access to their information and have a means to track and periodically audit any access to their information by others. Thus ensuring that customers have complete access to their health information at all times and that they exercise control over access to their information is key. Whether a customer's health information is stored as an electronic health record in a provider's information system or as an integrated personal health record in a common repository, it is important to address the ownership rights, control points, organizational liabilities, secondary uses, and potential risks of storing health information electronically.

Users should be made fully aware of the privacy policy that governs the system. The policy should provide all the details that enable users to make informed decisions regarding the use of their personal information. The policy should be easily available from anywhere on the site, and users should receive it when they register.

Agencies covered under the HIPAA guidelines are required by law to provide written notice of their privacy policies and practices to their customers. However, not all PHR vendors are regulated by HIPAA rules. Hence, at a minimum, consumers should have access to a clearly stated privacy policy before signing up for an online service. Secondary uses of their data, if any, should be fully disclosed. In addition, express consent should be obtained from customers before their personal health information is accessed or used for any purpose.

A Model for a Secure Online PHR System

An online PHR system's greatest advantage is accessibility. People with proper patient authorization may access the individual's health information from different locations. This authorized group can include family members, caregivers, primary care providers, specialists, pharmacists, and laboratories. Some may just view the information, while others contribute new information or update existing information.

The key to ensuring a system's security lies in fail-safe measures that prevent unauthorized access to an individual's information. Thus, ensuring proper authentication and access control is essential. Security measures should focus on securing information storage and preventing unauthorized access to the information.

In general, all online PHR systems should strive to follow certain standard security protocols and procedures. These include providing different levels of information access, enabling users to audit access to their information, publishing the security practices used by the system, maintaining audit logs, and offering functionality so that users can control access to their information.

A typical online PHR system consists of three key components:

- A secure central repository for storing patient information
- An online Web portal allowing users to view and maintain the information
- An optional interface to a provider's electronic system to enable real-time or batch transfer of data to a central repository to eliminate redundant data entry in two systems

The database, portal, and interface systems typically reside in a network infrastructure.

Network Infrastructure

Securing patient health information in an online system starts with securing the infrastructure that hosts and maintains the PHR system. These systems should be hosted in secure, state-of-the-art data centers that are reliable and scalable on demand. The data center should be protected with redundant cooling, raised floors, intelligent power, and generator backups. The facilities should be secured for authorized access with biometrics and smart-card controls. The network infrastructure and devices should be monitored constantly using the latest network operations monitoring tools and technologies.

The application and database-hosting environment should also be monitored using properly configured firewalls and intrusion detection systems. Periodic assessments should be conducted to include regular automatic scans of Internet devices for known security vulnerabilities, identification of potential weaknesses, assessment of network risks, and a tested plan for managing and mitigating infrastructure failure possibilities.

Data Repository

Relational databases have become the de facto standard for storing large amounts of interrelated information. The information in a relational database is logically organized into related tables representing various entities, each with their own unique set of attributes. For example, a patient demographics table will contain fields such as a patient's name, address, employment details, date of birth, and additional relevant personal information.

In an online PHR system, the information in the database is accessed via custom-developed applications or Web portals that have all the security and logic built into the application to control information retrieval. One common practice is to encrypt certain sensitive personal identifying information fields in the database so that if direct access is gained to the database tables,

key information is still protected. In addition to encrypting sensitive information, proper database security measures should ensure that information in the database tables is controlled and monitored for any unauthorized access.

PHR Web Portal

Transmission of information over the Internet should be secured using secure socket layer encryption, which will display to the user as an HTTPS connection. Access to the online PHR system should be controlled by a secure user ID and password. Passwords should be checked for their strength of security. It is recommended that passwords be at least eight characters long and contain a combination of letters, numbers, and symbols. Users should be prompted to change their passwords on a regular basis, and passwords should expire after a certain number of days.

Generally, different types of users have access to different portions of the portal. Also, certain users can only view the information, while others can add new information and update existing information. Detailed audit logs should be maintained of the successful and unsuccessful attempts to access a person's PHR and reported to the user and the system administrator.

More recent PHR systems offer advanced means of authenticating and controlling access to the system using a combination of personalized smart cards with additional biometric identification.

Online PHR systems are rapidly moving from a theoretical concept to an everyday reality. Given the sensitive nature of personal health information, regulatory laws like HIPAA and standards such as Health Level 7's are being established to ensure that an atmosphere and an associated infrastructure exist to enable patients and providers to exchange relevant health information in a secure and timely manner. These standards pertain particularly to electronic exchange of health data. This will ensure that disparate systems can talk to each other and exchange information in a common format. These standards and regulations must be kept in mind when designing reliable, scalable, and interoperable online PHR systems.

The security of an individual's personal health record is only as secure as the weakest link in the PHR system. Appropriate thought and planning must go into system design and development to ensure security and privacy while enabling easy access for authorized users. Systems that instill and guarantee consumer confidence can deliver the health benefits that PHRs offer.

Anil Srinivasan (anil@hdc4point.com) is the chief technology officer at HDC 4Point Dynamics in Omaha, NE.

Article citation:
Srinivasan, Anil. "Keeping Online Personal Records Private: Security and Privacy Considerations for Web-based PHR Systems" *Journal of AHIMA* 77, no.1 (January 2006): 62-63,68.

Driving the Power of Knowledge