

# Preventive Healthcare through Secure Personal Health Record Framework

Sangsuree Vasupongayya

Department of Computer Engineering, Faculty of Engineering  
Prince of Songkla University, Thailand

**Abstract.** A concept of personal health record (PHR) enables an individual to create, manage, and share his/her health information to a group of selected people through an online PHR management system. PHRs can contain home-monitored data and other health related information such as medical history, personal diseases, past allergic reactions, laboratory results, mental health information, physician diagnostic results and recommendations. Therefore, the data stored on the PHR is usually considered to be highly sensitive which raises a concern on the security of such data. In this work, the challenges in developing and deploying the secure PHR and some solutions to such challenges will be discussed.

**Keywords and phrases:** personal health record, preventive healthcare

## 1. Introduction

With the increasing healthcare cost, an alternative healthcare idea namely preventive healthcare has emerged. Preventive healthcare is an idea that emphasizes on monitoring a person condition and detecting a difference or a symptom in order to avoid a disease instead of curing the disease afterward. For example, an elder can capture his/her physiological responses from some wearable sensor devices and the information can be used later by the elder's physician. However, the data owner might not want his dietary details to be available to everyone; the data owner might not want the response from the physician on the wearable sensor device collected data to be available to his wife for some personal reasons. All these preferences must be respected by the framework or the system that stores such data. As part of the preventive healthcare solution, personal health records (PHRs) concept is introduced as an approach to store and share individual health related information on an online storage [1]. The owner of the PHRs has a full control over his/her information. That is the access to such data is controlled by an access control policy. This way, any person can collect

and store his/her health related information on an online storage and the data can be retrieved and viewed by an individual with the PHR owner permission.

## **2. Personal Health Records**

The PHRs concept allows any individual to create, collect, store and manage his/her health related information [1]. PHR is different from the electronic medical records (EMRs) and the electronic health records (HERs) concepts.

EMRs can be viewed as an electronic document of the patient's information sheet used by the physician at a healthcare institute [2]. EMRs contain notes and information collected by the physician or the laboratory staffs at the healthcare institute. Therefore, EMRs belong to the healthcare institute even though the EMRs contain the patient's information. Thus, the patient does not have any control over who can view his/her EMRs or when and how his/her EMRs will be used. Moreover, such EMRs are typically not sharable across healthcare institutes due to the different in the actual data formats and the management policies.

EHRs are focusing on making the EMRs available to more than one healthcare institute by storing the information related to the patient's clinical care. The information such as laboratory results and medical care history will be shared among authorized physicians from more than one institute. The main challenge of EHRs is dealing with various healthcare data structure standard such as CEN/ISO EN13606 [3], HL7 [4], and OpenEHR [5]. Even though EHRs are patient's centric in nature, the control over the EHR still does not belong to the patient. Thus, EHRs can be viewed as a partial EMRs portal for a set of authorized people.

The PHRs, on the other hand, is a framework used by the patients or regular people to maintain and manage their health related information in a private, secure and confidential environment [1]. Information inside the PHRs can be from various sources such as the patients themselves, the laboratory results, the health care providers, the physicians, the body sensor, and some health related applications. Important information of an individual can also be stored on the PHRs such as the medication lists, the allergy lists, the immunization histories, the emergency contact information, and the dietary plan. Moreover, the PHRs owner has a full control over his/her information by defining an access policy for an individual or a group of people. PHRs can be standalone or available online. However, this work will focus on the usefulness of the PHRs thus the PHRs must be available on an online storage. PHRs can be stored as plaintext format information. However, this work will focus on preserving the privacy of the PHRs owner and providing a security of the PHRs system. Therefore, the PHRs are stored in an encrypted form.

Existing PHRs systems include Indivo health platform [6], Microsoft HealthVault [7], Google Health [8], and the Australian government's PCEHR system [9].

### **3. Opportunities of PHRs**

Opportunities of PHRs can be discussed in 3 points including economical factor, technology factor, and global benefits.

PHRs allow an individual to monitor and update his/her health related information from their daily life activities such as exercise, nutrition, sleeping, medication, emotional feeling, actual vital signs, and symptoms that are happening. Such information can be a signal to indicate any irregular activity of the PHRs owner's body. By discovery the symptoms or diseases at an early stage, the healthcare cost can be reduced. Moreover, the possibility of curing the diseases is also high. From an economic point of view of the PHRs owner, the PHRs system can reduce the healthcare cost of an individual.

To be useful, the PHRs must be available for the users. With the current storage technologies and the current communication speed and bandwidth, the PHRs can be retrieved and uploaded from anywhere. The mobile penetration rate in many countries has been increasing rapidly in the past years. Since mobile users are potential PHRs users, the populations of these countries are potential PHRs users. Moreover, the rapid development of mobile technologies also provides an opportunity for the PHRs user as a smart device. Furthermore, the development of current mobile applications can be classified as potential PHRs collecting applications. For example, Health [10], which is an iPhone application, can automatically collect and store the physical fitness of its owner. Moreover, Health also provides some basic analysis information of the collected data. A personal health assistant on Android mobile device [11] is another application that allows its owner to input nutrition and exercise information while automatically collect the sleeping information of its owner.

With the current trends of populations in many countries, the world will move to an aging society in the next few years. PHRs can be viewed as a tool to provide a healthy aging society. If the world populations are aware of their health, these aging populations will be healthy and the global economic will not be interrupted. Not only the aging generation, the workforce generation can also benefit from the existing of a PHRs system. With the availability of the PHRs, the world is shrinking. Workforces can be moved from locations to locations and the PHRs will always be available to them.

### **4. Challenges in Deploying a PHRs System**

Many challenges exist in deploying a PHRs system. The challenges include the user acceptance, the PHRs service model, the local and global law and regulations and the user's right to privacy.

The user acceptance can be viewed as the acceptance among the PHRs users and the acceptance among healthcare personals. With the shifting work environment from paper-based to digital-based, majority of the workforces can used digital devices or familiar with using applications. Thus, the learning curve or the user acceptance might not be an issue. The main issue is the acceptance of

healthcare related persons, especially the doctors. Even though, the doctors are familiar with EMRs and EHRs. The doctors are still resisting to the PHRs idea because the owner of the data is the patients which is an unorthodox approach. However, the reliability of the information provided by the PHRs must be forced on the PHRs owner in order to reduce such issues. To be an owner of his/her health related data, the PHRs owner must collect the data himself/herself. Due to the various data formats and the data exchange methods, the method of collecting the health data must be done by the PHRs owner at this time. This action is possible at the present time because the patient can ask his/her physician to provide him/her with the details information of each visit. At this point, many people argue that such data will not be easy to understand by the PHRs owner because the information might be in the format of the doctor notations. This point is correct. However, the doctor notation can be read by another doctor. Therefore, the PHRs owner duty is to collect such data in order to have the data available for another doctor (if needed). Once the PHRs concept has been accepted, the method of having someone or an agent collects such data might be possible. Moreover, if the PHRs concept has been accepted worldwide, a method of transferring the data from various institutes might be possible. For example, The PCEHR system [9] is the Australian government national-scale project that provides a method to index various medical related information of a person from various places. To be accepted at the present time, the PHRs owner must be responsible for collecting and storing his/her data and the responsibility on using such data must be placed on the PHRs owner.

The PHRs service model is another issue in deploying a PHRs system. Typically, there are three models: government service model and non-government service model. The government service model is deployed in Australia under the Australian government's PCEHR system [9]. The PCEHR is a web-based national-scale e-healthcare system for all Australian citizens. The data stored on each healthcare organization will be indexing by the PCEHR system such that the records can be searched and retrieved as needed [12]. With the government service model, the management will be easier since the policy and the control will be decided by a single unit. An additional benefit of such model is the local law and regulations. Existing PHRs systems under a non-government service model include Indivo health platform [6] and Microsoft HealthVault [7] while Google Health [8] has been discontinued its service in 2011. Indivo health platform is a developer tool while Microsoft HealthVault provides a storage capacity for its users and provides an API for its users to exchange the stored data. Microsoft HealthVault has been developed on top of the Indivo health platform.

Since the PHRs system can service various users, the law and regulations of both local and global levels must aware of the existing of such system. Many local laws may enforce the privacy at different levels. How the PHRs system can be used and to what extend might depend upon the law and regulation of each location. The user's right to the privacy also faces the same issue. Moreover, the PHRs system must equipped with a method to track any inappropriate transaction in order to

ensure that only allowed transactions by authorized users are executed by the PHRs system. Moreover with a huge amount of auditing data, an efficient method to retrieve or analyze any inappropriate event must also be developed.

## **5. Challenges and Current Solutions in Developing a Secure PHRs Framework**

Challenges in developing a secure PHRs framework include an efficient encryption technology, an efficient policy management technique, an effective large data management, and a framework for special need such as an emergency situation.

An efficient encryption technology must be developed for PHRs system. Many PHRs systems use a database level encryption technique [6][7][8]. Since the PHRs system must be controlled by a policy, an attributed-based access control must be enforced. An attributed-based encryption technique such as ciphertext-policy attribute-based encryption technique (CP-ABE) [13] is utilized by various PHRs system [14][15][16] in order to provide a fine grain access control on the PHRs.

The policy management technique is required in order to ensure that each access to the PHRs is authorized and allowed by the PHRs owner. OAuth authorization framework [17] is applied in several PHRs systems in order to provide a fine-grained access control to a PHR owner. By employing CP-ABE the policy will be embedded with the encrypted data while the user with attributes defined in the policy can decrypt the data. This way, the policy is enforced by the encryption technique.

With the amount of PHRs data and the potential large number of PHRs users, the normal relational database management system might not be appropriate to store the PHRs. Therefore, the big data frame work for PHRs management must be developed. DSePHR [18] is a framework to modify existing big data framework namely HBASE [19] and Hadoop [20] to handle the encrypted PHRs data. Existing cloud storage for non-encrypted data includes MedCloud [21], Medoop [22], CHISTAR system [23] and Wiki-health system [24].

PHRs system might be used in special situation such as an emergency situation where the PHRs owner might be unconscious. Thus, the PHRs system must provide a feature to get an authorization for an emergency personnel to access some serious life-treading information such as the allergy lists. The work in [16][25][26] provides such features. The emergency server model is proposed in [25] and later extended to cover real situations in [16] while the work in [26] uses the PHRs owner fingerprint in a non-reversible format to identify the victims. Both works enable the PHRs system to be useful during an emergency situation while preserving the privacy of the PHRs owner. In addition, a two-level policy is proposed in [27] to allow the policy to be changed in order to support the delegation feature.

## 6. Conclusion

A concept of personal health record as a preventive healthcare approach to reduce the healthcare cost and providing a tool for an individual to monitor his/her condition and detect a difference or a symptom in order to avoid a disease instead of curing the disease afterward is discussed in this work. The discussion starts from providing the difference between the electronic medical records in any healthcare institute and the electronic health records which is an approach to partially share the EMRs among a set of authorized healthcare personals and the personal health records. Then, the discussion moves to the opportunities of the PHRs system in three points including an economic point of view, a technical standpoint and the global benefits of such system. In order to successfully deploy the PHRs system, many challenges must be faced include the user acceptance, especially the healthcare personals, the PHRs service model which can lead to the issue in the local and global law and regulations and the user's right to privacy. The last part of the work focuses on providing the challenges in developing a secure PHRs framework from four issues. These issues include an encryption technology, a policy management technique, an effective large data management, and a framework for special need such as an emergency situation.

Many large information technology companies such as Google and Microsoft have been involved in the PHRs applications for the past years. The Australian government conducts a national-scale project on such idea. Therefore, the PHRs concept is not new and many organizations have a touch on the idea. In addition, the rapid grow of computers, mobile devices and communication technologies will support the PHRs concept. Thus, the PHRs system will be on a list of daily application for users in the near future.

## References

1. P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption, *Journal of the American Medical Informatics Association (JAMIA)*, 13(2):121-126, 2006.
2. Office of the National Coordinator for Health Information Technology, "What are the differences between electronic medical records, electronic health records, and personal health records?", Internet: <https://www.healthit.gov/providers-professionals/faqs/what-are-differences-between-electronic-medical-records-electronic>, November 2, 2010, [11 March 2016].
3. The EN 13606 Association, "The CEN/ISO EN13606 standard", Internet: <http://www.en13606.org/the-ceniso-en13606-standard>, [11 March 2016]
4. Health Level Seven International, "HL7 Standard", Internet: <http://www.hl7.org>, [11 March 2016]
5. OpenEHR, "An open domain-driven platform for developing flexible e-health systems", Internet: <http://www.openehr.org/>, [11 March 2016]

6. Children's Hospital Informatics Program, "The Indivo Personally Controlled Health Record", Internet: <http://indivohealth.org/>, [11 March 2016].
7. Microsoft HealthVault, "HealthVault", Internet: <https://www.healthvault.com>, [11 March 2016].
8. Google Health, "Google Health – Google", Internet: [http://www.google.com/intl/en\\_us/health/about](http://www.google.com/intl/en_us/health/about), [11 March 2016].
9. PCEHR System in Australia, "My Health Record | Welcome to My Health Record", Internet: <http://www.ehealth.gov.au>, [11 March 2016].
10. Apple Inc, "iOS 9 - Health - Apple", Internet: <http://www.apple.com/ios/health/>
11. K. Anusornpakdee, M. Limpanadusadee, S. Vasupongayya, S. Kamolphiwong, "Personal health assistant on android mobile device: Sleeping, nutrition and exercise", *Advanced Materials Research*, volume 931-932, pp.1365-1369, 2014
12. C. Pearce, and M. Bainbridge, "A personally controlled electronic health record for Australia," *Journal of the American Medical Informatics Association (JAMIA)*, 21(4), 2014, pp. 707-713.
13. J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", 2007 IEEE Symposium on Security and Privacy (SP '07), 2007.
14. L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," *Proceedings of the 6th International Workshop on Wearable Micro and Nano Technologies for Personalized Health (pHealth)*, Oslo, June 2009, pp. 71-74.
15. C. Wang, X. Liu, and W. Li, "Implementing a personal health record cloud platform using ciphertext-policy attribute-based encryption," *Proceedings of the International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, Bucharest, September 2012, pp. 8-14
16. P. Thummavet and S. Vasupongayya, " Privacy-preserving emergency access control for personal health records", *Maejo Int. J. Sci. Technol.*, 9(01), pp. 108-120, 2015.
17. D. Hardt, "The OAuth 2.0 authorization framework", Internet Engineering Task Force Request for Comments 6749, Internet: <https://tools.ietf.org/html/rfc6749> October 2012, [September 13, 2015].
18. M. Wangthammang and S. Vasupongayya, "Distributed Storage Design for Encrypted Personal Health Record Data", *Proceeding of the 8th International conference on knowledge and smart technology (KST)*, Chiangmai, Thailand, 2016.
19. The Apache Software Foundation, "Apache HBASE", <https://hbase.apache.org/>
20. The Apache Software Foundation, "Apache Hadoop", <http://hadoop.apache.org/>
21. D. Sobhy, Y. El-Sonbaty, and M. Abou Elnasr, "MedCloud: Healthcare cloud computing system," *Proceeding of the 2012 Internet Technology and Secured Transactions*, pp.161-166, 2012.

22. W. Lijun, H. Yongfeng, C. Ji, Z. Ke and L. Chunhua, "Medoop: A medical information platform based on Hadoop", Proceeding of the 15th international conference on e-Health Networking, Applications & Services (Healthcom), 2013, pp.1-6.
23. A. Bahga and V.K. Madiseti, "A Cloud-based Approach for Interoperable Electronic Health Records (EHRs)," IEEE journal of Biomedical and Health Informatics, 17(5):894-906, 2013
24. L. Yang, L. Guo, C. Wu, C-H Lee and Y. Guo, "Building a cloud-based platform for personal health sensor data management," Proceeding of the 2014 IEEE-EMBS international conference of Biomedical and Health Informatics (BHI), pp.223,226, 2014
25. P. Thummavet, and S. Vasupongayya, "A novel personal health record system for handling emergency situations", Proceedings of the 17th International Computer Science and Engineering Conference (ICSEC), Nakorn Pathom, Thailand, 2013, pp. 266–271.
26. P. Choosang and S. Vasupongayya, "Using Fingerprints to Identify Personal Health Record Users in an Emergency Situation", Proceeding of the International Computer Science and Engineering Conference (ICSEC), Chiangmai, Thailand, 2015.
27. G. Wungpornpaiboon and S. Vasupongayya, "Two-layer Ciphertext-Policy Attribute-Based Proxy Re-encryption for Supporting PHR Delegation", Proceeding of the International Computer Science and Engineering Conference (ICSEC), Chiangmai, Thailand, 2015.