Secure Sharing of Personal Health Records in Cloud Computing

B. Raj Kumar[1], S. Satyanarayana[2]

[1]K L University, M. Tech (Computer Science), Vaddeswaram, Andhra Pradesh, India
batchurajkumar34@hotmail.com

[2]K L University, Associate Professor, Vaddeswaram, Andhra Pradesh, India
s.satyans1@kluniversity.in

Abstract: ***Personal health record, or PHR, is a health record where health data and information related to the care of a patient is maintained by the patient. This stands in contrast with the more widely used electronic medical record, which is operated by institutions (such as a hospital) and contains data entered by clinicians or billing data to support insurance claims. The intention of a PHR is to provide a complete and accurate summary of an individual's medical history which is accessible online. The health data on a PHR might include patient-reported outcome data, lab results, and data from devices such as wireless electronic weighing scales. Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. Existing Systems in the existing systems, the process uses revocable ABE algorithm. For each patient, the PHR data should be encrypted so that it is scalable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios.***

Keywords: PHR, patient-centric, Attribute Based Encryption

1. Introduction

There is currently no universal definition of a PHR, although several relatively similar definitions exist within the industry. In general, a PHR is an electronic record of an individual's health information by which the individual controls access to the information and may have the ability to manage, track, and participate in his or her own health care. A PHR should not be confused with an electronic health record (EHR). An EHR is held and maintained by a health care provider and may contain all the information that once existed in a patient's paper medical record, but in electronic form. PHRs universally focus on providing individuals with the ability to manage their health information and to control, to varying extents, which can access that health information. A PHR has the potential to provide individuals with a way to create a longitudinal health history and may include common information such as medical diagnoses, medications, and test results. Most PHRs also provide individuals with the capability to control who can access the health information in the PHR, and because PHRs are electronic and generally accessible over the Internet, individuals have the flexibility to view their health information at any time and from any computer at any location. The accessibility of health information in a PHR may facilitate appropriate and improved treatment for conditions or emergencies that occur away from an individual's usual health care provider. Additionally, the ability to access one's own health information in a PHR may assist individuals in identifying potential errors or mistakes in their information.

2. Types of PHRs

The PHR market continues to evolve at a rapid pace, with new types of PHRs continually emerging. For the purposes of this document, however, the universe of PHRs can be broken down into two categories: those subject to the Privacy Rule and those that fall outside of its scope. PHRs that are subject to the Privacy Rule are those that a covered health care provider or health plan offers. Examples of PHRs that fall outside the scope of the Privacy Rule are those offered by an employer (separate from the employer's group health plan) or those made available directly to an individual by a PHR vendor that is not a HIPAA covered entity. Some stand-alone software packages or portable devices also may be available for use by individuals as PHRs. However, while third parties may provide individuals with information to upload into these tools, since they are solely in the custody of the individual and are not offered by or connected to a third party, they will not be addressed in this document.

2.1 PHRs Offered by HIPAA Covered Entities

PHRs offered by HIPAA covered entities, such as health care providers or health plans, generally link individuals to, and allow them to view, some or all of the health records maintained about them within the covered entity. In many cases, an individual may not be given access to the entirety of his or her health record held by the health care provider or health plan and may only have the ability to view and not update or edit the information that is assembled by the health care provider or health plan. These PHRs also may allow individuals to add their own information into their PHRs and to update or edit this self-entered information. Many PHRs will include notations as

to the sources of information in the PHR, whether it be self-entered by the individual or entered by the health care provider or health plan. The individual may be able to control who else has access to the information in the PHR, such as, for example, a spouse, family member, or another health care provider.

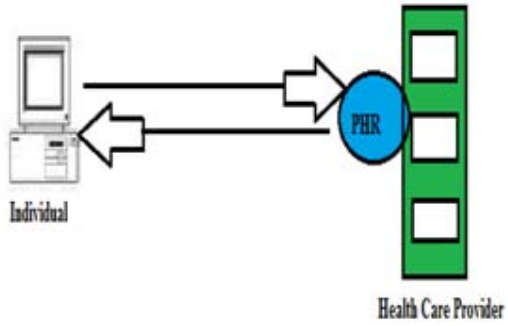

Figure 1: Information flow for PHRs offered by covered entities.

Information in the PHR flows between the individual and the covered health care provider or health plan that offers the PHR. Depending on the PHR; it may not be able to be accessed directly by outside entities. The health care provider or health plan stores the PHR and can update the information within the PHR. Information within the PHR is protected by the HIPAA privacy rule. The individual can access the PHR at any time and from any computer at any location.

2.2 PHRs Not Offered by HIPAA Covered Entities

The Privacy Rule does not apply to PHRs that are not offered by health plans or health care providers that are covered by the Privacy Rule. For example, PHRs may be offered by employers (separate from the employer's group health plan) or by PHR vendors directly to individuals. These types of PHRs are governed by the privacy policies of the entity that offers them, and in certain cases, may be governed by laws other than the Privacy Rule. However, the Privacy Rule still regulates how an individual's health information held by a HIPAA covered entity enters the PHR.

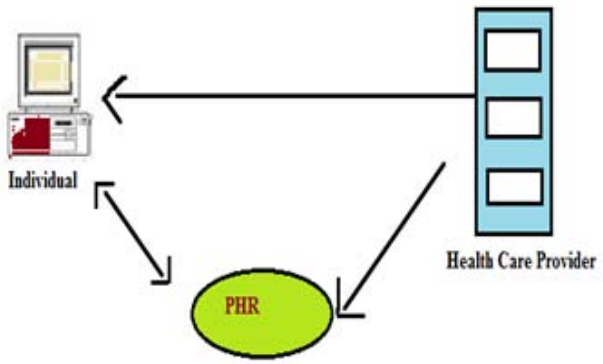

Figure 2: Information flow for PHRs not offered by covered entities

3. PHR architecture in Cloud

PHR architecture consists of three primary components: Data, Infrastructure and Applications. Data refers to the information that is collected, analyzed, exchanged and stored by different information technologies. Examples include medical history, laboratory and imaging results, list of medical problems, medication history, etc. Infrastructure is the computing platform which processes or exchanges healthcare data, such as software packages and websites. Applications include the data exchange, transactional, analytical and content delivery capabilities of the system, such as appointment scheduling, medication renewal, patient decision support system and disease education materials.

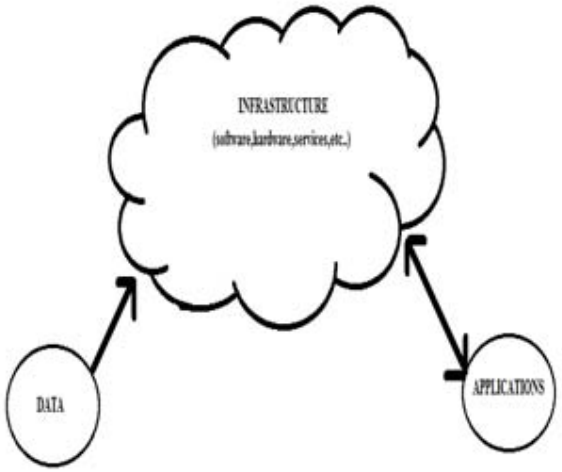

Figure 3: PHR cloud Architecture

4. Health Care Benefits from Cloud Computing

Cloud computing has the potential to revolutionize health care administration by allowing providers to access information from a patient's medical file at anytime from anywhere and that means patients receive better and more efficient quality care.

The 'cloud' is an intangible, but ubiquitous presence in our tech-laden lives, allowing health care professionals to access all patient data across multiple devices and from any location with an Internet connection.

As an IT strategy, cloud computing took the business world by storm, allowing companies to store massive amounts of data virtually, rather than making a huge investment in developing and maintaining their own information system storage. Yet, health care has been a relative latecomer to cloud computing, largely because of the industry's unique data security, regulatory, and patient privacy concerns.

As the move toward account able care organizations (ACOs) drives the need for a better flow of information between primary care providers, specialists and case managers, clinical use of the cloud is likely to expand to

include mobile applications that deliver data to tablets and smart phones. Most importantly, cloud-based platforms can allow collaboration between providers in real-time; from nearly any device that can connect to the Internet so health care organizations can manage data with more agility when working in the cloud.

5. Features

Cloud Computing is Ready for Personal Health Records:

Personal Health Records (PHRs) have the potential to enhance healthcare and reduce costs through better analysis and accurate diagnoses. According to experts, cloud computing and cost-effective information services can help realize the benefits of PHR.

Reduce the complexity of health informatics. Healthcare companies can learn lessons from the automotive industry, where automation introduced process management to gather and analyze data. Use regulation to improve healthcare
Standardized healthcare electronic systems provide clinical data to support doctors and researchers with information about the effectiveness of treatment.

Get a unified view with Clinical Data Repository (CDR). Hospitals and insurers alike can access consolidated data of patients with a CDR, enabling convenient and prompt analysis.

6. Conclusion

This study demonstrates overwhelming interest in the use of PHRs by patients, caregivers, and health providers alike. It also identified the features that have the best potential to engage patients, caregivers, and health care providers, and it supported previous research in the field. There was nearly universal interest in using the PHR regularly for accessing and exchanging health information, including medication, medical history reconciliation, and patient education and empowerment. It is recommended that a community-based implementation allow the PHR to be owned and controlled by the consumer and be portable among providers, plans, and employers to create high utilization. Future research is needed to determine the impact PHRs might have on actual health behaviors and health care costs and to address larger questions regarding financial issues of implementation and use, including documentation of cost savings and expenses related to PHR use.

References

[1] H. Lohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229
[2] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.
[3] "The health insurance portability and accountability act." [Online]. Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp
[4] "Google, Microsoft say hipaa stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/.
[5] "At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded," 2006. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/he-privacy26
[6] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," BMJ, vol. 322, no. 7281, p. 283, Feb. 2001
[7] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114.

Authors Profile

Batchu Rajkumar studying M. Tech (CSE) in K L University, He has published four international journal papers and presented research papers in 3 international conferences and received best paper awards in various conferences and member of SDIWC. My research on cloud computing, Business Intelligence and software engineering.

Dr. S. Satyanarayana is distinguished Scientist, Professor, Inventor, Author, and Business leader Born in India. He received his M. Tech (CSE) and PhD (Computational Mathematics) & PhD (Computer Science & Engineering) from Acharya Nagarjuna University & Capitol University and CMJ University. Dr. S. Satyanarayana early scientific work was mainly Graph Theory, Software Engineering, Cloud Computing Cryptography, SAS, Business Intelligence and Artificial Neural Networks. He Published More than 30 Research Papers & 3 Books in International Journals & Publications.