Journal of
Health & Medical Informatics

Achampong, J Health Med Informat 2014, 5:5
DOI: 10.4172/2157-7420.1000e127

Editorial Open Access

Readiness of Electronic Health Records for the Cloud Network

Emmanuel Kusi Achampong*

Department of Medical Education and IT, School of Medical Sciences, University of Cape Coast, Cape Coast, Ghana

Electronic Health Record (EHR) can be defined as the electronic record that stores patient's medical history information in a health record system, accessible and managed by both care providers and patients [1]. EHR has been in existence for over twenty (20) years now but its use has been restricted to few healthcare institutions due to high implementation cost and an unknown return on investment. The benefits of electronic health records (EHR) far outweighs that of paper records and thus makes it the obvious option for storing patient records. The high cost of EHRs and the little financial rewards are mentioned as the leading obstacle to adoption [2,3].

The issue of security and privacy of the EHR makes it unacceptable to patients. Centralised and distributed databases introduce the possibility to access large volumes of patient information in a short period. This also increases the chance of an unauthorised person accessing patient records easily. Acceptance of EHR solely depends on easy implementation, good security infrastructure and privacy settings.

As healthcare remains one of the most important and expensive sectors in any community, many technologies have emerged and been funded by governments and healthcare institutions to improve healthcare delivery outcomes. But EHR integration (the process of patient information sharing among healthcare providers and exchanging them over the internet with other healthcare providers) remains a challenge and a serious concern since it is exposed to theft, security violation, and standardisation difficulties [4].

Cloud computing technology is considered to be the new, most interesting and comprehensive solution in the information technology world. Its main objective is to leverage internet or intranet for users to share resources [5]. Cloud computing is a cost effective, automatically scalable, multitenant and securable platform that is managed by the CSP. NIST defines cloud computing as a model for enabling convenient, on-demand network access, to a shared pool of configurable computing resources, (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [6]. Cloud computing has four deployment models which are public, private, community and hybrid clouds.

A cloud computing present various benefits that makes the implementation EHR simple and easily accessible to all stakeholders. The definition of cloud computing make its importance clear as it seeks to present the benefits that goes with the uptake of the cloud network. The challenge with the cloud network since its inception has been its security infrastructure and how EHR will be secured from unauthorised users. The security of the EHR in the cloud settings is crucial since the cloud benefits also open it up for easy attack by hackers and crackers. It is therefore important to make the EHR at rest and in transition secured from all attacks in the cloud environment.

The upsurge of cloud computing opens a new chapter for healthcare delivery. The cloud computing model of network is based on the idea of subcontracting corporate information technology (IT) setup to other service providers, a distributed group of computer storage and computing network resources and facilities which becomes available quickly and on request. Benefits of cloud computing include easy and active resource provisioning, simple and automatic management of IT setups and the distribution of almost limitless CPU, storage space and bandwidth due to resource virtualisation, with upward enhancements and great cost discounts with respect to setup administration.

Several solutions can be developed to overcome the security concerns associated with EHR and cloud computing systems. However, progress to date has not been sufficient to meet the security requirements of a federated healthcare environment (cloud computing) [7]. Most of the information security models developed so far have been designed to satisfy healthcare security requirements in a controlled environment, such as the EHR database maintained within a hospital [8]. Current studies [8] focussed on encrypting and decrypting health records in a controlled environment without considering how encryption and decryption keys can be distributed in the cloud. Traditional access control mechanisms (Discretionary Access Control, Mandatory Access Control, Role-based Access Control and Task-based Access Control) have not been able to significantly secure health records in the cloud since each of them has a shortcoming that must be resolved to make it more robust to avoid unauthorised access and use.

It is important that researchers focussed their attention on what is termed advanced attribute-based access control and encryption in the cloud environment. This looks at innovative ways of sharing cryptographic keys in the cloud to unknown users of the EHR. It also focuses on advanced method of granting access to unknown users of the EHR in the cloud environment. This advanced attribute-based access control and encryption will lead to fine-grained security architecture for the EHR in the cloud computing environment. Until these security and privacy requirements are met, it will be unsuitable to implement EHR in the cloud computing environment.

References

1. Spil TAM, Katsma CP, Stegwee RA, Albers EF, Freriks A, et al. (2010) Value, Participation and Quality of Electronic Health Records in the Netherlands. 43rd Hawaii International Conference on System Sciences 1-10.
2. DesRouches C, Campbell E, Rao S (2008) Electronic Health Records in Ambulatory Care and National Survey of Physicians. N Engl J Med 50-60.
3. Jha A, DesRoches C, Campbell E, Donelan K, Rao S, et al. (2009) Use of Electronic Health Records in US Hospitals. N Engl J Med 10: 1628-1638.
4. Sun J, Fang Y (2010) Cross-domain Data Sharing in Distributed Electronic Health Record Systems. IEEE Transactions on Parallel and Distributed Systems 21: 754-764.

***Corresponding author:** Emmanuel Kusi Achampong, Department of Medical Education and IT, School of Medical Sciences, University of Cape Coast, Ghana, Tel: +233 (0) 242522445 and +233 (0) 206261849; Fax: +233 (0) 332138191; E-mail: e.k.achampong@uccsms.edu.gh; eachampong@ucc.edu.gh

Received February 05, 2014; **Accepted** February 07, 2014; **Published** February 14, 2014

Citation: Achampong EK (2014) Readiness of Electronic Health Records for the Cloud Network. J Health Med Informat. 5: e127. doi:10.4172/2157-7420.1000e127

5. Zhang L, Zhou Q (2009) Cloud Computing Open Architecture. IEEE International Conference on Web Services, Los Angeles, CA 607-617.

6. Mell P, Grance T (2011) NIST Definition of Cloud Computing. USA: National Institute of Standards and Technology.

7. Finance B, Medjdoub S, Pucheral P (2005) Privacy of Medical Records: From Law Principles to Practice. 18th IEEE Symposium on Computer-based Medical Systems 220-225.

8. AbuKhousa E, Mohamed N, Al-Jaroodi J (2012) e-Health Cloud: Opportunities and Threats. J. Network and Computer Applications 35: 211-220.