JES
Journal of Engineering Sciences

Vol 13, Issue 01, Jan /2022
ISSN NO:0377-9254

# Cloud-Based Electronic Health Records System (EHRS) Management

**[1]Dharavath Champla, [2]Dr. Siva Kumar**
[1]Research Scholar, Anna University
[2]Professor ECE Anna University

## ABSTRACT

*We describe a cloud-based strategy for the building of interoperable electronic health record (EHR) systems that may be used by many healthcare providers. Everyone involved in the healthcare ecosystem may profit from cloud computing platforms, which have a number of advantages (patients, providers, payers, etc.). In the transmission of healthcare data across multiple stakeholders, the absence of data interoperability standards and solutions has proven to be a significant impediment. This paper proposes an EHR system - cloud health information systems technology architecture (CHISTAR) - that achieves semantic interoperability through the use of a generic design methodology that employs a reference model that defines a general-purpose set of data structures and an archetype model that defines clinical data attributes. When developing CHISTAR application components, we use the cloud component model method, which consists of loosely linked components that interact asynchronously with one another. CHISTAR's high-level architecture as well as its approaches to semantic interoperability, data integration, and security are described in this document.*

## I. INTRODUCTION

It is estimated that up to 50,000 people die each year from influenza-like infections (ILI) in the United States (US) as a result of influenza. As a result, surveillance, early identification, and prediction of influenza epidemics are critical for the protection of the general population. Detection and surveillance systems for diseases give epidemiologic knowledge that enables health authorities to deploy preventative measures and assist clinic and hospital staff in the treatment of patients.

Administrators make the best options possible when it comes to personnel and inventory2.

The Centers for Disease Control and Prevention (CDC) in the United States monitors ILI in the country by collecting information from doctors' reports on individuals who have ILI and seek medical attention3. The Centers for Disease Control and Prevention's ILI data gives good estimates of influenza activity; however, it is only available after a one- to two-week time lag. This is a significant time gap, especially given the public nature of the work.

Health-related choices must be made on the basis of information that is more than two weeks old. A major need is the availability of systems that provide real-time estimations of influenza activity.

In recent years, several efforts have been made to develop methodologies that might provide real-time estimates of influenza activity in the United States by utilising Internet-based data sources that could possibly monitor ILI in an indirect way.

4,5,6,7,8,9,10,11. For example, Google Flu Trends (GFT), an Internet-based digital disease detection system that predicts influenza-like illness in the United States, has been the most commonly utilised of these non-traditional approaches in recent years12. As of August 2015, GFT was no longer in operation, creating an opportunity for fresh and dependable techniques to fill the void. More than a few lessons have been learnt in the area of digital illness identification through many upgrades to GFT that have been suggested not just by Google, but also by other researchers 13, 14, 15, 16, 17, 18, which have all been implemented. Including historical flu activity information as input and dynamically recalibrating the models have both enhanced the performance of some of these updated models, allowing them to not only integrate the most up-to-date clinical information but also respond to changes in population behaviour (for example, how Internet users search for health-related terms) 16,17,18. Finally, very accurate real-time ILI estimations may now be made available.

As illustrated in19, data streams from diverse sources in the United States may be combined to provide a national-level product.

In the case of flu estimates at the national level, it is difficult to transform them into actionable information that allows local health professionals to make better judgments during a spike in clinical visits, for example20. Therefore, more precise influenza predictions at finer geographical resolutions are preferable than less precise forecasts. Statistics from cities within the same geographical area tend to be positively associated when it comes to epidemiologic model parameters such as the basic reproduction number (R0), and these correlations are not consistent across regions in the United States (US)21. Additionally, when information of the influenza level in one area is combined with a network model derived from social network analysis, it has been shown that the accuracy of GFT's influenza-like illness (ILI) predictions may be improved both nationally and across numerous regions22. Unfortunately, the accuracy of current GFT-like systems degrades significantly at the regional and local resolutions23, as seen in Figure 1.

**Diverse studies have**

The excellent connection between aggregated data acquired from electronic health records (EHR) and flu syndromic surveillance systems24,25,26 has been shown retrospectively, indicating the viability of employing EHR data for illness monitoring at both local and regional geographic resolutions. In has been customary in the past for EHR data to be utilised for real-time monitoring owing to reporting lag periods of 1 to 2 weeks. This would be resolved if data from EHR records could be accessed in near real time.

The data collected and distributed in near real time by an electronic health records and cloud services company, athenahealth, when combined with historical patterns of flu activity using a suitable machine learning algorithm, can accurately track real-time influenza activity (as reported by the Centers for Disease Control and Prevention) at a regional scale in the United States, as demonstrated here. Furthermore, we demonstrate that the signal-to-noise ratio in this data source is quite high. We can get a "early count" of ILI activity from electronic health record data, in the same way that exit polls may be used to anticipate election outcomes. The data is utilised to create a machine learning model that is as timely as GFT used to be while also being steady and dependable as data sources approved by the Centers for Disease Control and Prevention (CDC). Despite the fact that our algorithm is capable of estimating influenza levels weeks in advance, we have opted to show here the real-time monitoring of ILI. Our model is designated as ARES, which stands for Autoregressive Electronic health record Support vector machine in computer science.

## II. LITERATURE STUDY

In cloud-based electronic healthcare (eHealth) systems, range query is an essential data search strategy for finding relevant information. It makes it possible authorised doctors to retrieve electronic health records as a target (EHRs) JinwenLiangaZhengQina...(2020), which are created and outsourced by patients from a cloud-based server In actuality, patients usually encrypt their electronic health records (EHRs) before outsourcing, making the range query impractical to perform. In this study, we outline three hazards that exist in the actual world.

**Cloud-Based Ehealth Systems,**

privacy invasion, frequency of use analysis, as well as the same data inference. In order to capture the security qualities that are resistant to these threats, we construct a security idea of indistinguishability under a multi-source ordered selected plaintext attack, which is defined as (IND-MSOCPA). After that, we recommend a multi-faceted approach.

Source order-preserving encryption (MSOPE) is a cloud-based eHealth system encryption solution that allows for range queries over encrypted EHRs from different patients to be performed. The MSOPE scheme is IND-MSOCPA secure, according to the results of the security study. Comprehensive performance reviews are also performed by the company, which indicate the great efficiency of the MSOPE programme. When it comes to providing eHealth services in various circumstances in an efficient and straightforward manner, cloud computing systems provide a fantastic potential. The scalability and mobility of the system

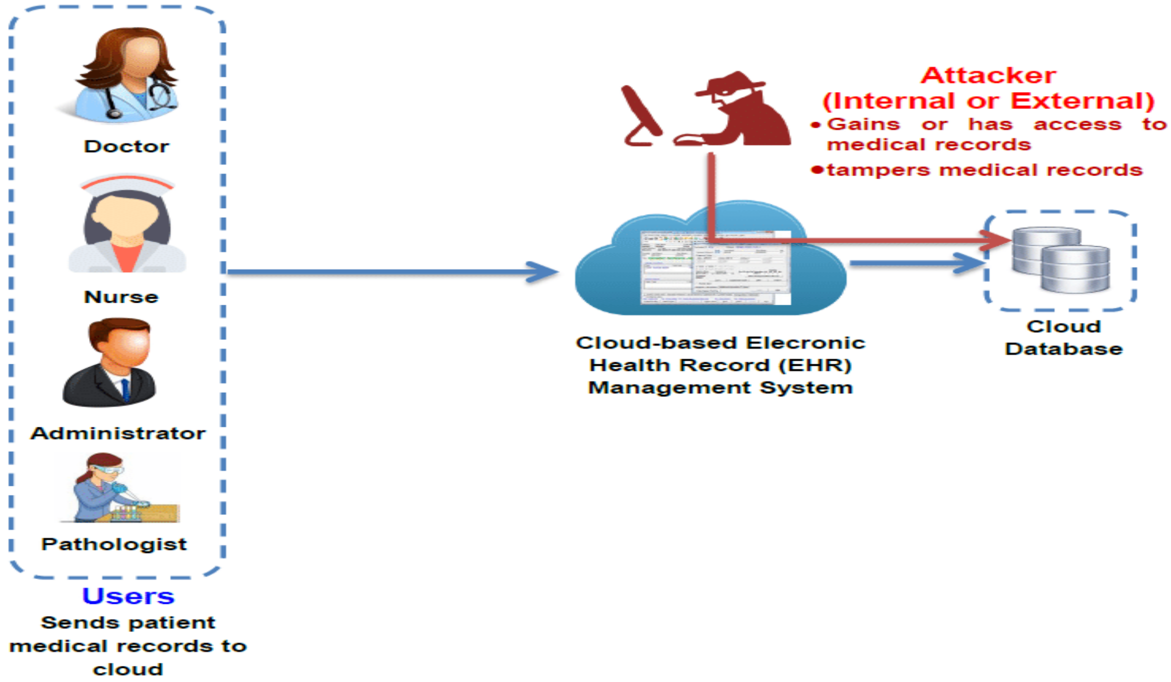
Doctor
Nurse
Administrator
Pathologist
Users
Sends patient medical records to cloud
Attacker
(Internal or External)
•Gains or has access to medical records
•tampers medical records
Cloud-based Elecronic Health Record (EHR) Management System
Cloud Database

FIG EHR

There are so many options for electronic health records that medical offices are finding it difficult to decide on a strategy.

Although it may seem to be a difficult and expensive process at first glance, it doesn't have to be. Web-based EHR solutions have proven to be the ideal answer for many small and medium-sized medical clinics.

Inquiring to see whether your workforce is well-suited to their duties. Looking for a way to keep your employees motivated and focused on the patient's needs and expectations? If you'd like a copy of our free e-book, "Staffing in the New Economy," please click here.

EHRs on the Cloud vs. Client-Server Systems

Cloud-based and client-server EHR systems are the two most common types. If you have an Internet connection, a cloud-based solution allows you to view your practice's data from any computer with an Internet connection.

Server, hardware, and software must be installed in a medical office to save data in a client-server system. Practices have typically relied on in-house servers, but this is changing due to a variety of factors.

Advantages of Using a Cloud-Based Electronic Health Record

EHR solutions that are hosted in the cloud make implementation considerably easier. There is no need to install any gear or software to operate EHR software since it runs on the web. With a considerably shorter installation procedure than conventional client-server solutions, practises may avoid interruptions to cash flow and increase returns on investment.

Practices save a significant amount of money by using EHR systems hosted in the cloud. For small medical practises, the initial cost of EHR installation is one of the biggest roadblocks. Just getting started with a client-server system may cost as much as $40,000, and that doesn't take into account the licence fees, maintenance expenditures, upgrades, and patches that follow.

It's cheaper to establish a cloud-based EHR since it doesn't need any hardware or software licencing. Software as a service (SaaS) is a subscription model in which practises pay a monthly cost, similar to a utility payment (SaaS).

Moving medical records to the cloud reduces the amount of IT resources needed by a large margin. In place of a staff of IT specialists, the SaaS provider does all of these tasks internally in the cloud, including installation, configuration, testing, running, security, and updating. In web-based systems, automatic updates ensure that procedures are executing on the most current version.

Users may safely enter into the system from wherever they have an Internet connection using web-based software, making it easier to collaborate than client-server systems. In a secure environment, doctors, employees, and patients can work together more efficiently in order to offer greater continuity of treatment, thanks to the ability to access the system from outside the office.

Cloud-based technologies make it easier to scale. Small practises don't have to go through the typical IT growth pains in order to expand. Adding additional users, providers, or locations is a breeze with an EHR system that is web-based. Online software's adaptability helps small firms to dream big and expand without going bankrupt.

Are Electronic Health Record (EHR) Systems Hosted on the Internet Safe?

The biggest issue of doctors who are sceptics of cloud-based EHR solutions is security. Web-based EHR solutions may really provide better security than client-server systems and paper records, despite the fact that doubt is natural.

EHR systems that are hosted on the web are HIPAA compliant since they are housed in secure data centres and use advanced encryption mechanisms that make the data unreadable even in the event of an attack or breach. Most client-server systems are not encrypted and only as safe as the storage room in which they are housed.

In the case of a natural catastrophe or fire, data stored in the cloud is more secure than data stored on paper or in client-server systems since the data is redundantly stored. In contrast to cloud systems, backups for client-server records are particularly subject to transfer to storage facilities.

Cloud storage has become the norm for many individuals, enabling them to save a significant amount of their personal information. Gmail and Yahooemail !'s systems are hosted on the cloud. Personal information on social networking sites like Facebook is also stored in the cloud.

Ultimately, cloud-based EHR systems provide users of all sizes and industries great advantages in cost savings, data accessibility, and security. Now, medical practices just have to be willing to look to the cloud for the future of healthcare IT.

There are various benefits [1-9] that a Cloud-based environment system may give, but there are also certain hurdles that must be addressed [10,11]. For example, in the instant The primary benefit of adopting a Cloud-based EHR management system is the capacity to exchange patient information with other clinical centres, as well as the integration of all the EHRs of a group of clinical centres in order to assist medical personnel in the performance of their tasks [12-14]. Consequently, how can health-care practitioners and clinical facilities ensure that their patients' data is kept secure, private, and confidential? For the Cloud computing paradigm to be successful in deploying a Cloud-based eHealth environment, the privacy and security of data moved to the Cloud must be the primary hurdle that must be surmounted. These responsibilities fall on both Cloud service providers and health care providers, since storing electronic health records (EHRs) on the Cloud demands a shift in thinking, and they must consider and manage all of the risks [15-17]. When a health care provider seeks to use a Cloud-based EHR management system, security concerns must be addressed immediately. The health care provider is responsible for guaranteeing the security of patient data by ensuring that the Cloud platform is equipped with the appropriate security features.. In order to prevent external assaults, it is also necessary to implement transmission and network secure protocols.

according to the data [18]. In the case of patient data, moving it to the Cloud implies that patient files are stored on the servers of the Cloud service provider [19]. What exactly does this imply? Unauthorized users must not be able to access or modify the information stored in these databases, hence it is critical that these organisations safeguard their databases. Because of the sensitivity of patient data, it is critical to be aware that when EHRs are transferred to the Cloud, privacy and confidentiality requirements must be included. In order to prevent unwanted access, cloud service providers must have authentication mechanisms that protect the confidentiality of medical information and safeguard patient privacy.

As a result of the Cloud Computing paradigm, eHealth systems now have the possibility to improve the features and functionality that they provide to patients (Joel JPC Rodrigues 1,Isabel de la Torre 2). Transferring patients' medical information to the Cloud, on the other hand, comes with a number of dangers in terms of the security and privacy of sensitive health information. In this study, the hazards associated with hosting Electronic Health Records (EHRs) on the servers of third-party Cloud service providers are discussed in further detail. Some recommendations for health-care professionals are provided in order to ensure the confidentiality of patient information while also making the procedure more efficient. Furthermore, the security risks that Cloud service providers should solve in their platforms are taken into consideration as well.

## III. RELATED WORK

The implementation of electronic health record management systems (EHRMS) is one of the most significant successes in eHealth in recent years. The use of these technologies is increasing at an alarmingly quick rate. In reality, this kind of technology is widely used in most industrialised nations, with a high degree of penetration. Under Spanish statute 41/2002, an electronic health record (EHR) is defined as documentation that incorporates information about the clinical progress of the patient throughout the course of his or her health aid procedure. The purposes of electronic health records (EHRs) are defined in this legislation, which also requires medical workers to protect the privacy of patients. According to Spanish legislation, this kind of material is classified as "specially protected" files. It is the goal of the 15/1999 legislation to establish this kind of nomenclature in order to protect the confidentiality of sensitive patient information. Except in the event of an emergency in which the patient's life is in danger, the patient's agreement is necessary in order to manage and access this information. HIPAA is a federal law that governs and specifies the security and privacy regulations for patient data in the United States. The Privacy Rule and the Security Rule are two portions of this legislation that are dedicated to preventing the inappropriate use of personal information: the Privacy Rule and the Security Rule. The HIPAA Privacy Rule states that Protected Health Information (PHI) must be made accessible in order to offer medical care to a patient, either with a court order or with the patient's agreement, according to the rule. This is a rule.

It also stipulates that businesses that make use of protected health information (PHI) must notify the patients of the usage of their PHI. The Privacy Rule also mandates that businesses with access to protected health information (PHI) utilise the smallest amount of patient data required to accomplish their purposes. Since its establishment in 2003, the HIPAA Security Rule has served as a supplement to the Privacy Rule, including many provisions to address the digitization of patient health information. The security assurances are divided into three categories: administrative, technological, and physical [23-25]. As a result, as previously said, health care providers must ensure and maintain the security and privacy of electronic health records, and then Implement the necessary security measures to ensure that patient information is kept secure in the Cloud. Firstly, we will discuss the security and privacy standards for patient records, followed by an explanation of the processes that a Cloud service provider must employ.

### Access Control on a Role-Based Basis

Access to the patient health record will be granted to a variety of different types of individuals. These range from those who are directly involved with the patient's care to those who are responsible for the maintenance of the provider's servers. It is possible that this data will be accessed by physicians, medical workers, or employees of the Cloud service provider. Because a doctor has access to patient data, a role-based access system is required to protect patient information.

Other technical people may have access needs for patient information that vary from those of other technical professionals. Identifying and assigning an ID code or number to each individual who has permission to access the stored information is necessary to resolve this issue. In accordance with the ID number, the user will be assigned to one of many groups, and each kind of group will have access to a certain portion of the patient information [22-26].

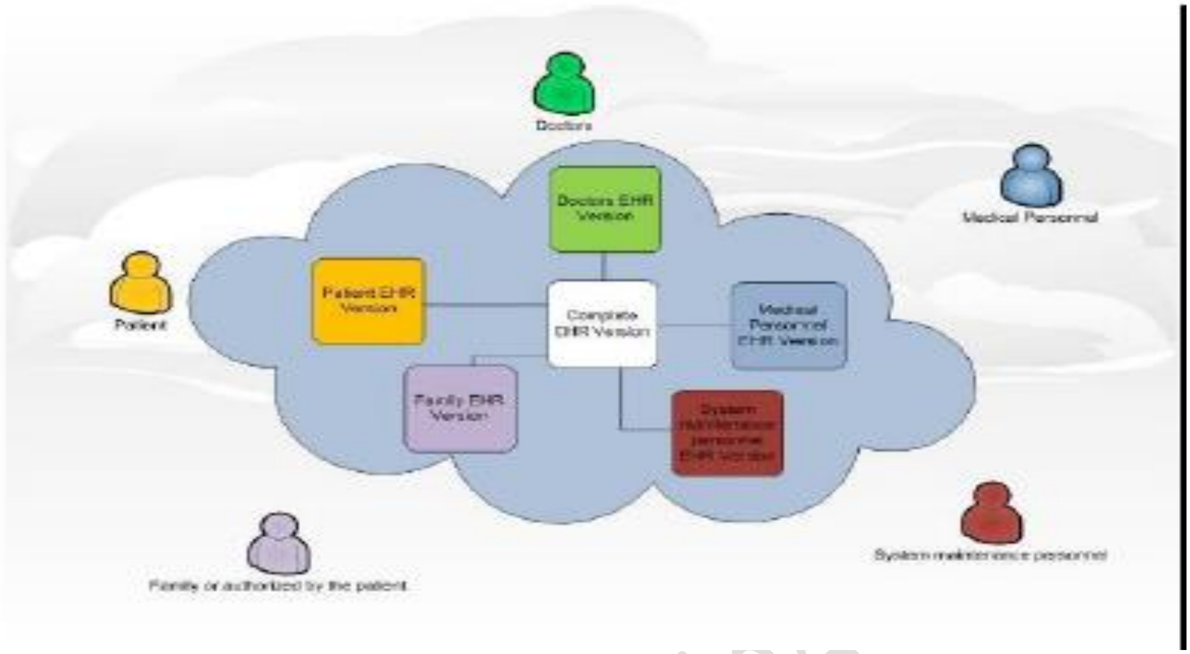
Doctors
Doctors EHR Version
Medical Personnel
Patient
Patient EHR Version
Complete EHR Version
Medical Personnel EHR Version
Family EHR Version
System maintenance personnel EHR Version
System maintenance personnel
Family or authorized by the patient

FIG PROPOSAL WORK

## IV. Proposal work

**Mechanisms for securing a network**

The information will most likely be at danger from sources "outside" of the Cloud platform. The staff of the service provider are not the primary danger that needs to be feared. It is critical to understand that by transferring patient data to the Cloud, health care professionals are exposing this information to a variety of external risks since the data is now accessible over the Internet [23]. As a result, it is the Cloud provider's obligation to preserve the security and privacy of the information by providing the necessary protection to prevent external intrusion.

assaults with the intent of stealing or possibly deleting information

**Data Encryption is a term that is used to describe the process of encrypting data.**

All sensitive patient information must be recorded securely in a private medical record in order for medical information to be shared across multiple physicians or medical workers while they are treating the patient. The information must be appropriately encrypted and regulated in order to ensure the security of this transaction.

**Digital Signature is a digital representation of a physical signature.**

In today's world, the digital signature is a highly valuable instrument that ensures the validity, integrity, and nonrepudiation of documents [14-15]. The validity of the digital record is ensured via the use of this security mechanism; it would be beneficial to deploy this kind of system in the Health Cloud in order to prevent the creation of fraudulent data transactions. The digital signature provides the receiver with the confidence that a message or file was delivered by the claimed sender even when the message or file is transferred via an insecure channel such as email. There are a plethora of cryptographic logarithms that may be used to implement this kind of security technology [23].

**Access to the system is being monitored.**

Every access to the platform should be tracked in order to compile a comprehensive list of all the individuals who have gained access to the system. In the event of an occurrence, the log may be used to solve or determine the reason of the issue. 111

the source of the issue It would be beneficial to keep a log of every update and modification made to each medical record. It is possible that moving electronic health records (EHRs) to the Cloud will be a significant step forward in the digitization of medical data. Scalability, a pay-per-use economic model, and the inclusion of the patient as an active participant in the health information management process are all factors that could lead to a shift in the way medical records are managed. When it comes to moving sensitive and private data to the Cloud, there are a number of considerations that must be taken into consideration. Security and data privacy are the most important of these requirements, and they are listed first. The privacy and security of patient health records are important considerations for Cloud service providers and health care providers when storing sensitive patient health record data in the Cloud. Those health-care providers, whether private or public clinical centres, who have made the decision to implement this kind of system must notify their patients about the changes in how their data will be maintained and kept in order to make this process as simple as possible. Additionally, the establishment of a trusting connection between the health-care professional and the Cloud service provider is critical to the success of this procedure. This confidence can only be established if the Cloud service provider can ensure that the necessary security measures are in place to preserve the confidentiality and privacy of the data being stored. A third-party organisation is involved. It was necessary to conduct an audit of the Cloud platform provider in order to demonstrate transparency in the management information system. It is possible that legislative procedures relating to data security will be crucial. Comparing the security policies of numerous cloud computing firms can be beneficial in determining which provider is the most appropriate for your needs.

## CONCLUSION

As a result of the rise of cloud computing, EHR management systems are undergoing a significant platform transition. However, such significant platform shifts must be treated with caution. Understanding all of the security criteria pertaining to the privacy and confidentiality of patient data is critical to ensuring a safe and seamless transfer. Even though the cloud computing paradigm is still in its early stages, it has the potential to be transformative in a wide range of sectors. More services and applications will be made accessible in the near future, and development will be accelerated.

## REFERENCES

1. *Furth B, Escalante A. Handbook of Cloud Computing 1st Edition. London: Springer; 2010.*
2. *Chen YY, Lu JC, Jan JK. A secure EHR system based on hybrid clouds. J Med Syst 2012 Oct;36(5):3375-3384. [CrossRef] [Medline]*
3. *Low C, Hsueh Chen Y. Criteria for the evaluation of a cloud-based hospital information system outsourcing provider. J Med Syst 2012 Dec;36(6):3543-3553. [CrossRef] [Medline]*
4. *Poulymenopoulou M, Malamateniou F, Vassilacopoulos G. Emergency healthcare process automation using mobile computing and cloud services. J Med Syst 2012 Oct;36(5):3233-3241. [CrossRef] [Medline]*
5. *Buyya R, Ranjan R. Special section: Federated resource management in grid and cloud computing systems. Future Generation Comput Syst 2010;26(8):1189-1191.*
6. *Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A. A view of cloud computing. Commun ACM 2010;53(4):50-58.*
7. *Anderson NR, Lee ES, Brockenbrough JS, Minie ME, Fuller S, Brinkley J, et al. Issues in biomedical research data management and analysis: needs and barriers. J Am Med Inform Assoc 2007;14(4):478-488 [FREE Full text] [CrossRef] [Medline]*
8. *Svantesson D, Clarke R. Privacy and consumer risks in cloud computing. Comput Law Secur Rev 2010;26(4):391-397.*
9. *Fernández-CardeñosaG, De la Torre-Díez I, López-Coronado M. Rodrigues JJPC.Analysis of cloud-based solutions on EHRs systems in different scenarios. J Med Syst 2012;36(6):3777-3782.*
10. *Fernández-Cardeñosa G, De la Torre-Díez I, Rodrigues JJPC. Analysis of the Cloud Computing Paradigm on Mobile Health Records Systems. In: Proceedings of the Sixth International Conference on*

*Innovative Mobile and Internet Services in Ubiquitous Computing. 2012 Presented at: Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing; July 2012; Palermo, Italy.*

11. *De la Torre-Díez I, Díaz-Pernas FJ, Fernández-Cardeñosa G, Antón-Rodríguez M, Martínez-Zarzuela M, González-Ortega D, et al. Analysis of the benefits and constraints for the implementation of Cloud Computing over an EHRs system. In: Proceedings of the 6th Euro American*
12. *Conference on Telematics and Information. 2012 Presented at: 6th Euro American Conference on Telematics and Information Systems; May 2012; Valencia, Spain.*
13. *Yellowlees PM, Marks SL, Hogarth M, Turner S. Standards-based, open-source electronic health record systems: a desirable future for the U.S. health industry. Telemed J E Health 2008 Apr;14(3):284-288. [CrossRef] [Medline]*
14. *Blanchet KD. Electronic health records: are consumers riding or driving the car? Telemed J E Health 2008 Apr;14(3):210-214. [CrossRef] [Medline]*
15. *Hargreaves JS. Will electronic personal health records benefit providers and patients in rural America? Telemed J E Health 2010 Mar;16(2):167-176. [CrossRef] [Medline]*
16. *Piette JD, Mendoza-Avelares MO, Ganser M, Mohamed M, Marinec N, Krishnan A preliminary study of a cloud-computing model for chronic illness self-care support in an underdeveloped country. Am J Prev Med 2011 Jun;40(6):629-632. [CrossRef] [Medline]*
17. *HIPAA General Information. URL: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/index.html?redirect=/HIPAAGenInfo/ [accessed 2013-07-10] [WebCite Cache]*
18. *Tejero A, de la Torre I. Advances and current state of the security and privacy in electronic health records: survey from a social perspective. J Med Syst 2012*
19. *Oct;36(5):3019-3027.*
20. *Saquero-Rodríguez A, De la Torre-Díez I, Durango-Pascual A. Análisis de Aspectos de Interés sobre Privacidad y Seguridad en la Historia ClínicaElectrónica. Revistaesalud.com 2011;7(27).*
21. *Zhang R, Liu L. Security Model and Requirements for Healthcare Application Clouds. In: Proceedings of the IEEE 3rd International Conference on Cloud Computing. 2010 Presented at: IEEE 3rd International Conference on Cloud Computing; July 2010; Miami, Florida.*
22. *Cloud Computing: Top 5 Security Concerns. 2012 Feb 23. Health Information Technology, Implementation, Insight, News, Spotlight, Today URL: http://www.ehrscope.com/blog/cloud-computing-top-5-security-concerns/ [accessed 2013-07-10] [WebCite Cache]*
23. *Amazon Web Services:Overview of Security Processes. 2011 May. URL: http://d36cz9buwru1tt.cloudfront.net/pdf/AWS_Security_Whitepaper.pdf [accessed 2013-07-10] [WebCite Cache]*
24. *Force.com Security Resources. URL: http://wiki.developerforce.com/page/Security [accessed 2013-07-10] [WebCite Cache]*
25. *Fledel Y. Google Android: A Comprehensive Security Assessment. IEEE Security & Privacy 2013 (forthcoming). [CrossRef]*