Original Paper

Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems

Joel JPC Rodrigues[1*], BSc, MSc, PhD; Isabel de la Torre[2*], BSc, MSc, PhD; Gonzalo Fernández[2], BSc; Miguel López-Coronado[2], BSc, MSc, PhD

[1]Instituto de Telecomunicações, University of Beira Interior, Covilha, Portugal

[2]University of Valladolid, Valladolid, Spain

[*]these authors contributed equally

Corresponding Author:
Joel JPC Rodrigues, BSc, MSc, PhD
Instituto de Telecomunicações, University of Beira Interior
Rua Marques D'Avila e Bolama
Covilha, 6201-001
Portugal
Phone: 351 275242081
Fax: 351 275319899
Email: joeljr@ieee.org

Abstract

Background: The Cloud Computing paradigm offers eHealth systems the opportunity to enhance the features and functionality that they offer. However, moving patients' medical information to the Cloud implies several risks in terms of the security and privacy of sensitive health records. In this paper, the risks of hosting Electronic Health Records (EHRs) on the servers of third-party Cloud service providers are reviewed. To protect the confidentiality of patient information and facilitate the process, some suggestions for health care providers are made. Moreover, security issues that Cloud service providers should address in their platforms are considered.

Objective: To show that, before moving patient health records to the Cloud, security and privacy concerns must be considered by both health care providers and Cloud service providers. Security requirements of a generic Cloud service provider are analyzed.

Methods: To study the latest in Cloud-based computing solutions, bibliographic material was obtained mainly from Medline sources. Furthermore, direct contact was made with several Cloud service providers.

Results: Some of the security issues that should be considered by both Cloud service providers and their health care customers are role-based access, network security mechanisms, data encryption, digital signatures, and access monitoring. Furthermore, to guarantee the safety of the information and comply with privacy policies, the Cloud service provider must be compliant with various certifications and third-party requirements, such as SAS70 Type II, PCI DSS Level 1, ISO 27001, and the US Federal Information Security Management Act (FISMA).

Conclusions: Storing sensitive information such as EHRs in the Cloud means that precautions must be taken to ensure the safety and confidentiality of the data. A relationship built on trust with the Cloud service provider is essential to ensure a transparent process. Cloud service providers must make certain that all security mechanisms are in place to avoid unauthorized access and data breaches. Patients must be kept informed about how their data are being managed.

(J Med Internet Res 2013;15(8):e186) doi: 10.2196/jmir.2494

KEYWORDS

cloud-computing; eHealth; electronic health records (EHRs); privacy; security

Introduction

Cloud computing environments provide a great opportunity to provide eHealth services in different scenarios in an effective and simple way. The scalability and mobility that a Cloud-based environment system can offer provides several advantages [1-9], but there are some barriers that must also be managed [10,11]. In the case of deploying a Cloud-based EHR management system, the main advantage is the ability to share patient records with other clinical centers, and the integration of all the EHRs of a group of clinical centers in order to help medical staff perform their jobs [12-14]. So, how can health care providers and clinical centers guarantee the security, privacy, and confidentiality of their patients' data? The privacy and security of data migrated to the Cloud represents the main barrier that the Cloud computing paradigm must overcome if a Cloud-based eHealth environment is to be deployed. This mission must be performed by both Cloud service providers and health care providers, since hosting EHRs in the Cloud requires a change of approach and they must take into account and address all these risks [15-17].

Security issues are critical when a health care provider plans to deploy a Cloud-based EHR management system. The health care provider must guarantee the security of patient data by ensuring that the Cloud platform has the needed security mechanisms in place. Transmission and network secure protocols also must be deployed in order to avoid external attacks to the data [18]. Moving patient data to the Cloud means that patient files are hosted in the servers of the Cloud service provider [19]. What does this mean? It is essential that these companies ensure the security of their databases so that the data cannot be accessed or modified by unauthorized users. It is important to be aware that privacy and confidentiality terms are essential when EHRs are migrated to the Cloud because of the sensitivity of patient data. In order to avoid unauthorized access, Cloud service providers must deploy authentication systems that ensure the privacy of patient information.

Governments must require that Cloud service providers fulfill the privacy requirements needed to ensure the privacy of patient data. The deployment of a legal framework will help to accomplish a secure environment [13,14]. Privacy policies have been legislated in several countries in order to regulate and safeguard the privacy of patient records. As an example, the US Health Insurance Portability and Accountability Act (HIPAA) regulates the privacy and security of US patient data [20]. These policies depend on each country. Furthermore, EHRs themselves are ruled by standards, which include security and privacy terms, such as Health Level 7 (HL7) [21,22], to guarantee data security and privacy. By combining these standards with Cloud policies and security mechanisms implemented by providers, a secure "Health Cloud" scenario will be achieved.

This paper addresses the health care providers' security and privacy issues that must be considered when deploying EHR management systems. Taking into account these issues on both sides, the migration process will be more secure and transparent. Some security mechanisms necessary to deploy a proper solution are suggested.

We will first elaborate on the issues and requirements for maintaining the security and privacy of EHRs. After that, we explain the requirements that a Cloud-based EHR management system must guarantee in terms of security. Also, some suggestions are given to health care providers in order to facilitate the process.

Methods

For the analysis and study of Cloud-based EHR systems, we reviewed published papers and research about security and privacy issues, which different Cloud computing providers use for development of their Cloud platforms. The related literature was obtained mainly from Medline sources. Direct contact with some Cloud service providers was made. Many publications that show the feasibility of Cloud computing implementations for eHealth services were reviewed in order to look for the latest information on this emerging technology. Most of them show the advantages that Cloud-based solutions can provide to eHealth systems.

Results

Electronic Health Record Security and Privacy Issues

The deployment of EHR management systems is one of the most important achievements in eHealth in recent years. The implementation of these systems has been growing rapidly. In fact, most developed countries have a high level of penetration of this kind of system.

According to Spanish law 41/2002, an EHR is defined as the documentation, which contains information about the clinical evolution of the patient during his or her health assistance process. In this law, the uses of EHRs are set out, requiring medical personnel to maintain the privacy of patients. The Spanish law treats this kind of information as "specially protected" files. This kind of nomenclature is set in the 15/1999 law with the purpose of guarding the privacy of sensitive patient information. The patient's consent is required to manage and access this data, except in the case of an emergency where the patient's life is at risk.

In the United States, HIPAA regulates and establishes the security and privacy requirements of patient data. This law includes two sections on avoiding the improper use of personal information: the Privacy Rule and the Security Rule. The HIPAA Privacy Rule establishes that the Protected Health Information (PHI) must be made available in order to provide the patient medical treatment, either with a Court order or with the authorization of the patient. This rule adds that the entities that use the health information must notify the patient about the use of their PHI. Furthermore, the Privacy Rule requires that entities accessing the PHI use the least amount of patient data necessary to meet their needs. The HIPAA Security Rule was set in 2003 and complements the Privacy Rule, adding several terms to address the digitalization of the patient health information. It has three kinds of security guarantees: administrative, technical, and physical [23-25].

Thus, as outlined above, health care providers must guarantee and preserve the security and privacy of EHRs, and then implement the required security mechanisms to keep patient information safe in the Cloud. Before explaining the mechanisms that a Cloud service provider must implement, we describe the security and privacy requirements of patient records.

Electronic Health Record Security and Privacy Requirements

Before moving EHRs to the Cloud, the EHR systems themselves must set several guarantees to preserve sensitive patient information. The combination of these security requirements with those of the Cloud systems will guarantee the privacy and security of EHRs hosted in the Cloud. The requirements to secure an EHR are described in Table 1 [22]. The security and privacy issues that a Cloud-based system must address in order to safeguard patient files are analyzed in the next section.

Security and Privacy Issues of Cloud-Based Health Solutions

Deploying Cloud-based health solutions is an important step in the development of eHealth. Cloud-based systems allow the ability to create scalable environments, which are adapted to user needs. This total adaptation is complemented by the savings offered by a pay-per-use system, like Cloud computing. Another great advantage comes from the fact that, when EHRs are hosted in the Cloud, medical personnel or patients have the ability to access the information at any time from wherever they have an Internet connection. Currently, with the global economic crisis, saving money could be one of the most important reasons that would drive a company to move its electronic health system into the Cloud. Therefore, Cloud service providers must take advantage of this fact when selling their prospective clients on the advantages of Cloud-based systems.

In order to guarantee the security of their systems, Cloud service providers must install several security mechanisms to keep the safety, privacy, and security of their clients' data. In the section below, we explain the different mechanisms that a Cloud service provider implements in its systems to maintain the security of files in the context of EHR security.

eHealth Cloud Security Issues

A Cloud-based EHR must maintain the same level of data security as data stored in the servers of the health care provider. Patients and medical personnel should know that their personal information is going to be stored with a third-party provider; the provider must guarantee the same security and privacy that the EHRs had in the local servers. The patient, obviously, is not involved in the process of moving their sensitive information to the Cloud, but information should be communicated to patients by the health care providers about the data migration. These communications are not simple notifications; instead, patients should be informed about all the advantages that a Cloud-based system offers for the management of their medical information. Patients should know that data management responsibility lies with both parties: the Cloud service provider and, in a more active way, the health care provider or clinical center. However, there are security issues that should be considered by both providers and customers of a Cloud-based EHR system.

Table 1. Requirements for maintaining the security and privacy of an electronic health record.

Requirements	Description
Authorized access	In order to deploy an authorized-control system, it is essential to deploy an identification system for both patients and health care providers. This identification must be portable between the different entities that have access to the patients' data. This system might be achieved by the ID identifier of each patient. Regarding the authentication, a centralized system based on a public key is viable. A RBAC (Role-Based Access Control) should be deployed in order to allow authorized personnel access to specific data based on their role.
Confidentiality	To guarantee the confidentiality of the communication process, encryption algorithms are used. However, the confidentiality problem in a distributed system arises because it is not possible for the information transmitter system to verify that confidentiality has not been exposed on the receiving end.
Patient's consent	According to the legislation, patients must allow or deny access to their clinical information, except in emergency situations. This consent could be implicit or explicit. Another fact to consider is the need to get access to the EHR-hosted entity from another external one. This process should have the consent of the patient, but in case of emergency, a security mechanism must be provided to avoid this restriction without the patient's consent.
Relevance	All the medical personnel who take part in the diagnostic and treatment process have access to the EHR. Administrative personnel will be able to access the clinical information if their function is relevant to the medical process. Therefore, only the relevant personnel will get access to the patient information. To guarantee that only this level of personnel has been able to access the data, an access control system must be deployed. Given the difficulty of establishing information relevance, it is preferable to have a default permission access and, if necessary, study possible abuses.
Information ownership	The ownership of the EHR is not clearly established. The medical personnel are responsible for this information. However, the patients themselves have the right to access their clinical information.
Information consistency	In an interoperability outline, a correction notification mechanism must be created in order to show changes to the information. This system must allow access to the previous versions of the EHRs, if necessary.
Audits	An audit register should include all accesses to the information and all the changes that have taken place to the EHRs. This system allows the monitoring of access and is a powerful tool to guarantee a secure system. This audit system should fulfill the interoperability requirements.
Archiving	Medical records should be archived for a set period of time, according to the legislation of the respective country. After this period of time, the medical data may be deleted. However, this is not recommended when it comes to EHR management and practice, where the aim is to keep the complete medical information about the patient for his or her lifetime. However, from a logistical standpoint, this would have massive long-term storage requirements.

Role-Based Access

There are many different kinds of personnel who will have access to the patient health record, from the patients themselves to the technicians responsible for the management of the provider's servers. Physicians, medical personnel, or employees of the Cloud service provider could have access to these data. To ensure the privacy of the patient data, a role-based access system is needed because a doctor may have different access requirements to the patient information than other technical personnel. In order to overcome this problem, an ID code or number must be assigned to each person allowed to access the stored information. Depending on the ID number, the user will belong to a group and each kind of group will have access to a certain part of the patient information [22-26]. For example, patients and doctors will get access to the entire health record whereas the personnel responsible for maintenance of the platform will be able to access only the information they need for proper system operation. With this role-based system, the patients' privacy is relatively guaranteed. Figure 1 illustrates the different roles that could take part in a Health Cloud and the different versions they will have access to.

Network Security Mechanisms

The main risk to the information will likely be "outside" the Cloud platform. The provider personnel are not the main threat that has to be feared. It is important to know that when moving patient data to the Cloud, health care providers are exposing this information to several external threats because the data are now available via the Internet [23]. Therefore, the responsibility must lie with the Cloud provider itself to protect the security and privacy of the information by providing the security needed to avoid external attacks to steal or even delete the information.

Data Encryption

All sensitive patient information must be stored securely in a private medical record so that medical information can be shared by different doctors or medical personnel. In order to secure this transaction, the information must be properly encrypted and controlled.

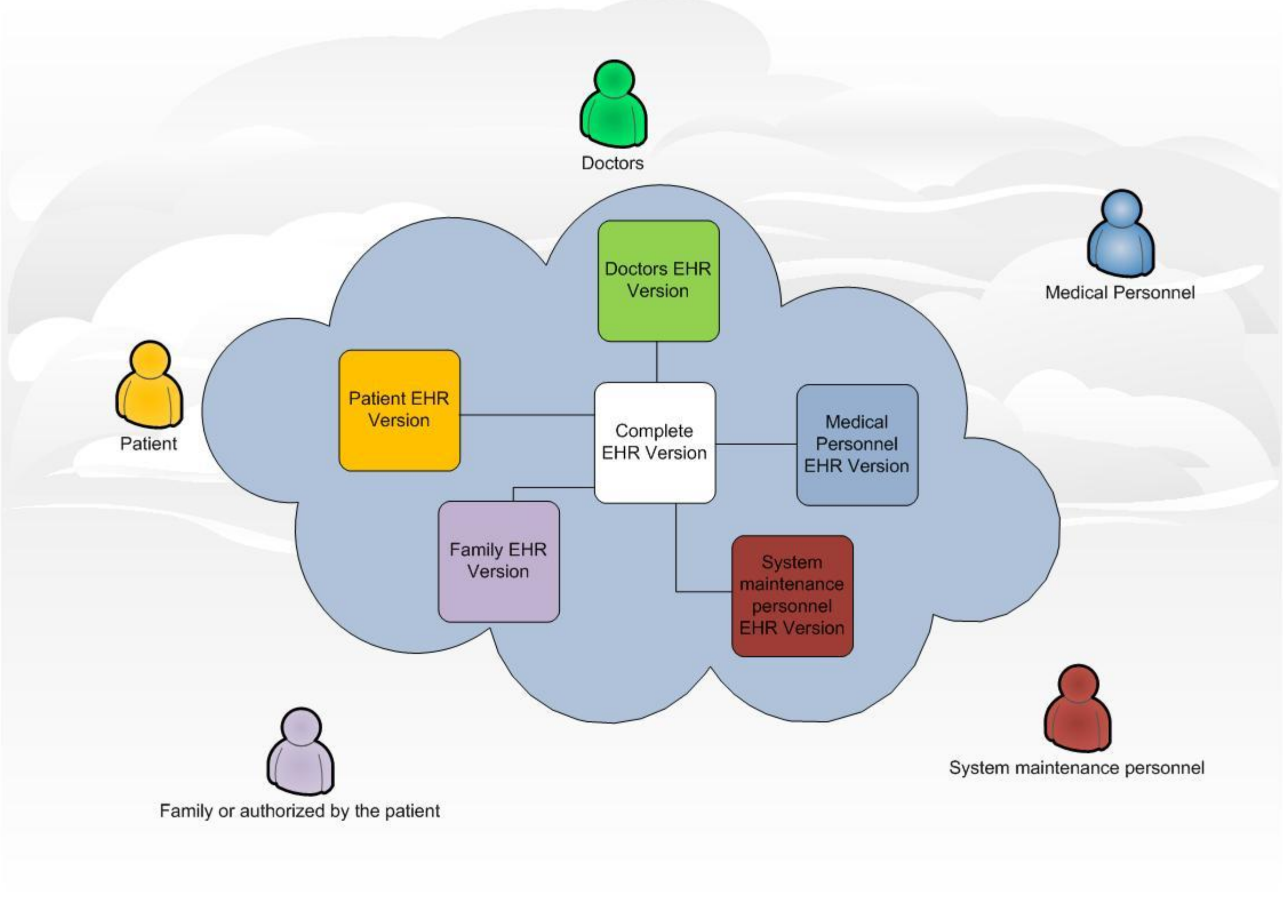
Digital Signature

The digital signature is a very useful tool that provides authenticity, integrity, and nonrepudiation [14-15]. With this security mechanism, the authenticity of the digital record is guaranteed; it will be valuable to deploy this kind of system in the Health Cloud in order to avoid false data transactions. For messages sent through an unsecure channel, the digital signature gives the receiver the reassurance that a message or file was sent by the claimed sender. There are many cryptographic logarithms to deploy this kind of security tool [23].

Monitoring of System Access

Every access to the platform should be monitored in order to create a log of all the people that have had access to the system. In case of an incident, the log can be consulted to solve or find out the cause of the problem. It would be valuable to create a log to track every update and change to each medical record [23].

Figure 1. Role-based system with different electronic health record versions available depending on the kind of user of the Health Cloud.


Doctors
Medical Personnel
Patient
Doctors EHR Version
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

Suggestions Before Moving Electronic Health Records to the Cloud

The main worries of health care providers planning to move patient information to the Cloud are data security and privacy. Migrating data to the Cloud means that a third party now has control over the Cloud-hosted data. In order to address the risks that could arise, Cloud clients should be well informed before moving data to the Cloud. In order to facilitate this process, the Cloud service provider's customers themselves should be informed about the services the Cloud provider offers them and the security mechanisms installed on the provider's servers. Cloud clients should demand total transparency from the Cloud service provider. Knowing this kind of information is critical to being able to choose the most suitable provider for the client's needs. Table 2 shows several security issues a client should consider when choosing the most appropriate provider [21].

Moving Electronic Health Records to the Cloud: Example of a Cloud Company's Security Requirements

Health care providers that decide to move their EHRs to the Cloud should be aware of these kinds of security mechanisms before migrating their records. There are several well-known Cloud service provider companies, for example, Amazon Web Services, Microsoft Cloud, GoGrid, or Salesforce, with similar security terms as explained below. Thus, this section is useful in the case of choosing a Cloud service provider. Based on the security deployed on several Cloud platforms, we suggest the following mechanisms to secure the Cloud system [22,26,27].

Third-Party Certification

In order to guarantee the safety of the data and meet the requirements of privacy policies, the Cloud provider must be compliant with various certifications and third-party requirements (see Table 3).

Monitoring

The provider should include automated monitoring tools to provide a high level of service performance and system availability. These tools should be available online for internal and external use.

Notification alarms can be configured when any modification of the data is made by the maintenance personnel or the users themselves. These tools will help track all the information changes made to the stored cloud data. Any kind of incident with the stored data will be monitored.

Information and Communication

In order to use the Cloud platform as a communication channel where personnel could be notified and kept up to date on everything that happens, the Cloud provider should employ various methods of internal communications in order to help employees to understand their roles and responsibilities, and to communicate significant events, if necessary. These communication methods could include orientation and training programs for newly hired personnel, video conferencing, and email, among others.

Employee Lifecycle

Several policies are established in the Cloud platform to manage user access. The Cloud service provider should require that staff with potential access to the patient data undergo an extensive background check (as permitted by law) commensurate with their position and level of data access. Some of these policies are shown in Table 4.

Physical Security

The data center building should be strictly controlled and secured with video surveillance, expert security staff, intrusion detection systems, and other electronic means. The authorized personnel should pass through authentication controls to access the data center floors.

Environmental Safeguards

Innovative architectural and engineering approaches should be used in database centers so as to avoid external agents that could damage them (see Table 5).

Configuration Management

The company should communicate all updates on both the infrastructure and the software itself, so as to minimize any impact on the customer and the service. The software updating process should be designed to avoid unintended service disruptions and maintain the integrity of service to the customer. Before updating software, these updates should be reviewed, experimented, and approved. The Cloud provider staff would manage the data center infrastructure and be responsible for the hosting management, system scalability, availability and auditing, and security management.

Business Continuity Management

The Cloud service provider must guarantee the availability of the service offered. In order to ensure system availability and continuity, the company should address the security issues considered in Table 6.

Backups

In order to guarantee the existence of the patient data stored in the Cloud, the provider should redundantly store these data. Multiple backups of these data should be stored in different data centers in various locations.

Storage Service Decommissioning

When a Cloud storage service comes to the end of its useful life, the provider should guarantee that data previously stored there is completely removed from its servers. Furthermore, the provider must ensure that unauthorized personnel have not copied these data.

Network Security

The platform itself is not the only element that should be secured by the provider. The Cloud provider must also secure the network. The network provider should guarantee significant protection against traditional network security issues, such as those summarized in Table 7.

Table 2. Suggestions before moving electronic health records to the Cloud.

Security issues	Description
Data security	Because a Cloud provider will have access to all the information concerning the patients, project plans, etc, it is essential to check the provider's reputation in the market. The provider must guarantee that its clients' information would not be misused by any unauthorized personnel. The health care provider should check for the data protection and operational integrity services offered by the provider. Moreover, it is valuable to know the geographic location of the servers where the client data would be hosted. In brief, clients should demand total transparency.
Regulatory compliance	It is important to choose providers with security certifications and are ready for external audits. It is crucial that the provider guarantee the continuity of the service in case the provider has some kind of problem. The client must ensure that the provider operates in the country where the service will be offered. Data logging and data monitoring are important tools that Cloud providers should offer in order to improve the security of the service.
User authentication	Because the data are processed externally by a third party, there is always some inherent risk. The client must know about the personnel who will manage the medical information and what standards for access will be followed by the provider. The client must be informed about the role-based access systems as well as the password handling system configured by the provider.
Data separation	The provider not only handles the data stored in the Cloud but manages the data of other companies who have hired its services. So it is important to know the mechanisms the Cloud provider implements to separate the data of all the companies that are sharing the same servers. The clients must be informed about the availability of the data that the provider guarantees.
Legal issues	A legal framework must guide the policies of the Cloud provider. Intellectual property rights agreements between the two parties should be of prime importance. While the provider owns the right to its infrastructure and applications, the client owns the right to his/her data and computational results.

Table 3. Third-party certifications of the Cloud provider.

Certification	Brief overview
SAS70 Type II	Statement on Auditing Standards No 70: Auditing statement that provides guidance to service auditors when assessing the internal control of a service organization and issuing a service auditor's report.
PCI DSS Level 1	The Cloud provider should be certified with the PCI Data Security Standard as a shared hosting service provider.
ISO 27001	Certification of the Information Security Management System (ISMS) that covers infrastructure, data centers, and service terms.
FISMA	Certification to operate at Federal Information Security Management Act (FISMA) Low Level, which is a US federal law enacted in 2002. It recognizes the importance of information security to the economy and national security interests of the United States.

Table 4. Employee lifecycle policies of a Cloud provider platform.

Policy	Brief overview
Account provisioning	The Cloud provider itself assumes the responsibility of provisioning employees and contractor access. This access to the resources hosted in the Cloud platform must be explicitly approved by the owner or data manager.
Account review	Every access account is reviewed in Cloud platforms every 90 days.
Access removal	Every employee's access account is automatically revoked when it is concluded.
Password policy	Access to the platform is performed by user IDs and passwords to authenticate users to services, resources, and devices, as well as to authorize the appropriate level of access to each user.

Table 5. Environmental safeguards installed in data centers.

Safeguard	Brief overview
Fire detection and suppression	Automatic fire detection and suppression systems are installed in the data center rooms to remove the risk of fire.
Power	24/7 electrical power systems that guarantee the uninterruptible running of the service.
Climate and temperature	In order to prevent overheating of the servers, climate control is required. This is a critical concern for the data center management and consumes lots of energy.
Management	Monitoring systems to control the state of the database equipment.

Table 6. Business continuity management.

Term	Brief overview
Availability	Data centers are built in clusters per regions. In case of failure of one of these data centers, automated processes move the client data traffic away from the affected area.
Incident response	Technical support and coverage to solve any kind of problem 24/7/365 (24 hours a day, 7 days a week, and 365 days a year) must be offered.
Company-wide executive review	A Cloud company should be periodically audited and supported by an internal audit group.

Table 7. Protection against network security issues.

Security network issue	Overview
DDoS attacks	Distributed Denial of Service (DDoS) mitigating techniques is included in the Amazon Web Services (AWS) platform to avoid this kind of attack.
MITM attacks	Man In The Middle (MITM) attacks are avoided because all the endpoints of AWS are secured by Secure Socket Layer (SSL), which provides server authentication.
IP spoofing	Traffic platform is controlled by a firewall infrastructure. Then the stored data cannot send spoofed network data.
Port scanning	Unauthorized port scans by customers are a violation of the provider’s use policy. Every reported violation should be investigated.

Discussion

Principal Findings

Migrating electronic health records (EHRs) to the Cloud may represent a great step in the digitalization of medical data. Advantages like scalability, economic model of pay per use, and involving the patient as an active part of the health information management process may assume a change of model in the management of medical records. Several requirements must be taken into account when the time comes to migrate sensitive and private data to the Cloud. Of those requirements, security and privacy of data are the most important ones. In storing the sensitive data of patient health records, Cloud service providers and health care providers must ensure the privacy and confidentiality of the Cloud-hosted data. In order to make this process easier, health care providers, either private or public clinical centers, that have decided to deploy this kind of system, must inform their patients of the change in how their data will be managed and stored. Additionally, a relationship of trust between the health care provider and the Cloud service provider is an essential factor in this process. In order to achieve this trust, the Cloud provider must guarantee that the security mechanisms are in place to protect the security and privacy of the stored data. An external company is needed to audit the Cloud platform provider in order to show transparency in the management information process. Legislative mechanisms regarding the security of data may be important. Comparing the security terms of several cloud computing companies will be valuable in order to choose the most suitable provider.

Conclusion

With the emergence of Cloud computing, EHR management systems are facing an important platform shift, but such important changes must be approached carefully. In order to make a secure and smooth transition, studying all the security requirements regarding the privacy and confidentiality of patient data are essential. The Cloud computing paradigm is still under development but stands to become revolutionary in many different fields. In the near future, more services and apps will be available, and development will be enhanced.

Acknowledgments

This research has been partially supported by the Spanish Social Security Administration Body (IMSERSO) under the project 85/2010, by the Instituto de Telecomunicações, Next Generation Networks and Applications Group (NetGNA), Portugal, by National Funding from the FCT—Fundação para a Ciência e a Tecnologia through the Pest-OE/EEI/LA0008/2013 Project, and by the AAL4ALL (Ambient Assisted Living for All), project co-funded by COMPETE under FEDER via QREN Programme.

Conflicts of Interest

None declared.

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. [doi: 10.1007/s10916-012-9830-6] [Medline: 22351166]

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. [doi: 10.1007/s10916-012-9829-z] [Medline: 22366976]
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. [doi: 10.1007/s10916-011-9814-y] [Medline: 22205383]
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. Bateman A, Wood M. Cloud computing. Bioinformatics 2009;25(12):1475.
7. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A. A view of cloud computing. Commun ACM 2010;53(4):50-58.
8. Creeger M. CTO roundtable: cloud computing. Commun ACM 2009;52(8):50-56.
9. Kuo AM. Opportunities and challenges of cloud computing to improve health care services. J Med Internet Res 2011;13(3):e67 [FREE Full text] [doi: 10.2196/jmir.1867] [Medline: 21937354]
10. 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] [doi: 10.1197/jamia.M2114] [Medline: 17460139]
11. Svantesson D, Clarke R. Privacy and consumer risks in cloud computing. Comput Law Secur Rev 2010;26(4):391-397.
12. 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.
13. 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.
14. 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 Conference on Telematics and Information. 2012 Presented at: 6th Euro American Conference on Telematics and Information Systems; May 2012; Valencia, Spain.
15. 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. [doi: 10.1089/tmj.2007.0052] [Medline: 18570554]
16. Blanchet KD. Electronic health records: are consumers riding or driving the car? Telemed J E Health 2008 Apr;14(3):210-214. [doi: 10.1089/tmj.2008.9982] [Medline: 18570543]
17. Hargreaves JS. Will electronic personal health records benefit providers and patients in rural America? Telemed J E Health 2010 Mar;16(2):167-176. [doi: 10.1089/tmj.2009.0063] [Medline: 20082592]
18. Coles-Kemp L, Reddington J, Williams PAH. Looking at clouds from both sides: The advantages and disadvantages of placing personal narratives in the cloud. Information Security Technical Report 2011;16:115-122.
19. Piette JD, Mendoza-Avelares MO, Ganser M, Mohamed M, Marinec N, Krishnan S. 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. [doi: 10.1016/j.amepre.2011.02.014] [Medline: 21565655]
20. 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 ID 6I11USrUj]
21. 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 Oct;36(5):3019-3027. [doi: 10.1007/s10916-011-9779-x] [Medline: 21947856]
22. Saquero-Rodríguez A, De la Torre-Díez I, Durango-Pascual A. Análisis de Aspectos de Interés sobre Privacidad y Seguridad en la Historia Clínica Electrónica. Revistaesalud.com 2011;7(27).
23. 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.
24. 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 ID 6I11rOzss]
25. 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 ID 6I11tBPdk]
26. Force.com Security Resources. URL: http://wiki.developerforce.com/page/Security [accessed 2013-07-10] [WebCite Cache ID 6I11uoLos]
27. Fledel Y. Google Android: A Comprehensive Security Assessment. IEEE Security & Privacy 2013 (forthcoming). [doi: 10.1109/MSP.2010.2.]

Abbreviations

AWS: Amazon Web Services
DDoS: Distributed Denial of Service
EHR: Electronic Health Record
FISMA: Federal Information Security Management Act
HL7: Health Level Seven
HIPAA: Health Insurance Portability and Accountability Act
ISMS: Information Security Management System
MITM: Man In The Middle
PHI: protected health information
SSL: Secure Socket Layer

Edited by K El Emam, G Eysenbach; submitted 15.12.12; peer-reviewed by J Lloret, P Lorenz, C Monteiro; accepted 11.06.13; published 21.08.13

Please cite as:
JPC Rodrigues J, de la Torre I, Fernández G, López-Coronado M
Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems
J Med Internet Res 2013;15(8):e186
URL: http://www.jmir.org/2013/8/e186/
doi: 10.2196/jmir.2494
PMID: 23965254