Health Records on the Cloud: A Security Framework

Miloslava Plachkinova, Ala Alluhaidan, and Samir Chatterjee
Center for Information Systems and Technology, Claremont Graduate University, Claremont, CA, USA

Abstract - The current study investigates the process of selecting a cloud service provider for implementing an electronic health record (EHR) system on the cloud from a security standpoint. This is an important issue because many eligible physicians still do not use EHRs and thus cannot meet the meaningful use criteria and receive incentives provided by the Centers for the Medicare and Medicaid Services (CMS).

To facilitate the process of selecting a cloud provider, we propose a framework focusing on the security issues related to implementing EHR systems on the cloud. The framework targets evaluators from healthcare practitioners and is designed to be a comprehensive tool for improving decision-making. The current study contributes to the literature as it utilizes design science methods to healthcare information systems and provides an overview of the current state of EHR, cloud computing, and security. The study also discusses many practical implications and recommendations for healthcare.

Keywords: Healthcare, Security, Cloud Computing, Management, Decision Support, Design Science Research

1 Introduction

Modern healthcare has relied on technology as one of its pillars to success. Electronic health record (EHR) systems can improve the quality of care through clinical monitoring and by reducing rates of medical errors [1]. EHRs can also add value to medical practices by improving the clinical decision support systems [2]. Countless systems and applications exist to meet the needs of healthcare professionals and the vast amounts of data which they collect and store on the cloud [3]. This creates an enormous potential threat of undesired access to this information, or the even more worrisome possibility of patients being intentionally harmed [4]. Cloud computing plays a significant role in the EHR implementation process because it improves the interoperability and access to information at minimal costs [5].

Security is an essential factor for every EHR system on the cloud [6]. Currently, the Centers for the Medicare and Medicaid Services (CMS) provide incentives for medical practitioners who are willing to participate in the process of implementing EHRs to achieve meaningful use. However, most eligible physicians still do not have EHR systems that demonstrate the meaningful use criteria [7] and thus cannot take advantage of the offered incentives. One reason for this problem can be selecting a particular vendor or multiple vendors for implementing the EHR system. Currently, there are over 600 certified vendors [8] and choosing the right one presents a difficult task for many medical practices.

Even though selecting a vendor is a challenging issue, not much has been done in regards to addressing the medical practitioners’ needs and to offering them practical advice on how to securely implement an EHR system onto the cloud. EHR implementation may come in two forms: (1) Vendors provide software and all the collected data resides within the medical facility; or (2) Vendors provide a web front-end but all processing and data is done remotely on the cloud. Prior literature review addresses in great detail cloud computing, healthcare information systems, and security as separate disciplines, but little research has been done on how to properly integrate them together. This lack of integration has led to significant difficulties when a decision has to be made in regards to the security of EHRs on the cloud. In spite of past research [9], there is still a great need for a practical sequence of steps to complete or check when selecting a suitable vendor that provides EHR services on the cloud.

This paper proposes a design science artifact, a security framework, which can be used by medical practices as they proceed on making a decision to implement an EHR system on the cloud. This framework summarizes the current state of research on cloud computing, healthcare IS, and security while providing healthcare professionals with a better process in selecting a cloud service provider (CSP).

Following main design science principles [10, 11], we aim to develop an online survey to evaluate the usefulness of the framework. The survey is planned to be distributed to healthcare providers. Overall, we consider the proposed artifact to be a useful tool for small-to-medium medical practices when selecting a CSP for health records on the cloud. A pilot study is also planned to provide constructive feedback to improve the effectiveness of the tool and to suggest barriers to implementing EHR systems on the cloud.

2 Related Work

Healthcare information systems have been extensively investigated by researchers [12-14]. Prior studies have clearly outlined the benefits of implementing such systems and their positive impact on the overall healthcare quality [15, 16]. These studies indicate that the potential of information
technology (IT) is far reaching in regards to how it can improve the existing hospital workflow and reduce medical errors and administrative efforts. It is difficult, especially for smaller medical practices, to keep pace with the latest trends in technologies. Financial limitations and a lack of resources also contribute to this trend. This is why finding a good process to select CSP can increase the success of such healthcare practices and can improve overall performance. For the purposes of this paper we use the classification of medical practices in terms of size (small, medium and large) as suggested by [17].

Clouds is defined as “large pools of virtualized resources which can be adjusted to a variable load scale and are exploited by a pay-per-use model.” [18] Thus, it allows for the incorporation of technologies into medical practices in an efficient manner [18]. According to the National Institute for Standards and Technology (NIST), there are five main characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [19].

Private clouds can be used by a single practice where there is greatest control over the data and network. Public clouds are available to the general public but they provide no control. Hybrid clouds are a combination of both and they address most of the issues of each approach [20].

Also, there are three types of cloud services classifying the degree of control over the provided services. Software-as-a-Service (SaaS) offers no control to the client. Platform-as-a-Service (PaaS) grants control to subscribers. Infrastructure-as-a-Service (IaaS) offers strictly limited control to the deployed application and operating systems [21]. Clouds provides easy access to resources without requiring significant initial investments [22]. This is useful for small medical practices that do not have the capacity to build and support the required infrastructure. Yet, there is a lack of sufficient technical expertise and resources to choose the right CSP by Small-to-midsize practices.

Security of healthcare information systems requires specialized knowledge and experience, and practitioners in small-to-midsize practices may be unfamiliar with all the requirements and compliance issues. Research has been conducted in the past with regards to the security aspect of information systems [23]. However, the topic may be overwhelming for many medical professionals who lack the necessary expertise in the IT area. Healthcare security is also an aspect that researchers have focused on [24], and yet many questions remain unanswered. Some of them include: ensuring privacy and security of personal health records (PHR), overcoming barriers to adoption of PHR, and achieving meaningful use. Since many medical practices are emerging within the United States, securing patient information is one of the highest concerns to be addressed.

Healthcare cloud security has been investigated in the past without proposing viable solutions for it. Researchers have identified healthcare security issues and applications of cloud computing [25], security and privacy concerns [26], and requirements [27]. This trend explicitly demonstrates the need for a solution to the secure implementation of EHR systems on the cloud.

3 Security Framework

The current paper proposes a security framework for health records on the cloud (Figure 1). This framework can be an efficient tool for small-to-medium healthcare for a better vendor selection process [28].

The framework is developed in accordance with design science principles suggested by [10, 11] to ensure its utility and usefulness. The framework we propose consists of five phases and represents a flow which can be successfully applied in the decision making process of selecting a cloud provider.

3.1 Phase I: Requirements

Phase I consists of evaluating the technical capabilities of the CSP, and of financial and management analyses needed before committing to cloud services provider. These main principles have been identified in prior literature [29] to be of significant influence to the process of implementing EHR records on the cloud.

CSP needs to be carefully evaluated considering role-based services, so that only authorized personnel will have access to the necessary data and thus the problem of privilege abuse will be addressed [30]. The CSP also needs to provide secure user identification for monitoring and auditing access logs [31]. It is known that Cloud identity management is a challenge considering that data should be accessible easily regardless of location or device with a maintainable level of authenticity that is not obstructed by multiple methods of authentication. Centralized authentication with a single strong password is one way to address the previous challenge and provides a method for provisioning and de-provisioning [32]. Auditing logs can be used as evidence in an eventual investigation in cases of compromised data. Next, CSP’S ability to provide sufficient capacity for the healthcare practice is of key importance. One of the main reasons for companies to use cloud services is the need for scalability. That saves them money and improves service costs in the long term. The CSP should be able to demonstrate capacity and data encryption. What mechanisms it uses to encrypt the data, how is the process being done, does it require public key infrastructure (PKI) or other encryption models? These are just some of the questions the medical practice needs to ask before committing to a contract with a specific CSP. In addition, securing the deletion of the data oftentimes, if not done properly, and can lead to data leakages or thefts. Monitoring system access should be done only by authorized individuals with verified credentials. The CSP needs to demonstrate clear backgrounds on all of its employees to reassure the integrity of its operations. Network security is
Figure 1. A Security Framework for Health Records on the Cloud

<table>
<thead>
<tr>
<th>Phase I: Requirements</th>
<th>Financial Analysis</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Capabilities:</strong></td>
<td><strong>Cost:</strong></td>
<td><strong>Business continuity:</strong></td>
</tr>
<tr>
<td>Role-based access;</td>
<td>Cloud model;</td>
<td>Systems integration;</td>
</tr>
<tr>
<td>User identification;</td>
<td>Cloud service model;</td>
<td>Workflow compatibility;</td>
</tr>
<tr>
<td>Capacity planning;</td>
<td>Hidden costs;</td>
<td>HR needs</td>
</tr>
<tr>
<td>Data encryption;</td>
<td>ROI</td>
<td></td>
</tr>
<tr>
<td>Secure data deletion;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring system access;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network security;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile security;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data center security</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Go with CSP?** NO

**Phase II: Service Level Agreement**

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Data Ownership</th>
<th>Patient Consent</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA-compliance;</td>
<td>Data use and access;</td>
<td>Inform patients;</td>
</tr>
<tr>
<td>HL7 standard;</td>
<td>Data return process;</td>
<td>Obtain consent;</td>
</tr>
<tr>
<td>HIE standards;</td>
<td>Data physical location;</td>
<td>Additional security</td>
</tr>
<tr>
<td>Certifications and accreditations;</td>
<td>Privacy;</td>
<td></td>
</tr>
<tr>
<td>Insurance;</td>
<td>Liability;</td>
<td></td>
</tr>
<tr>
<td>Data breach and violation;</td>
<td>Data mining</td>
<td></td>
</tr>
<tr>
<td>Data sovereignty guarantee</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Go with CSP?** NO

**Phase III: Cloud Implementation**

<table>
<thead>
<tr>
<th>Pilot Implementation</th>
<th>Testing</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review other implementations;</td>
<td>Thorough testing;</td>
<td>Before and after trainings;</td>
</tr>
<tr>
<td>Feedback from clients;</td>
<td>End-users and agents of change;</td>
<td>Monitor workflow processes;</td>
</tr>
<tr>
<td>One system at a time</td>
<td>Feedback;</td>
<td>Feedback from providers and patients;</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>User manuals</td>
</tr>
</tbody>
</table>

**Go with CSP?** NO

**Phase IV: Evaluation**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Health Standards</th>
<th>Security Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benchmarks;</td>
<td>HIE;</td>
<td>HIPAA security rule;</td>
</tr>
<tr>
<td>Best practices;</td>
<td>Direct;</td>
<td>User standards;</td>
</tr>
<tr>
<td>Security audits</td>
<td>Connect;</td>
<td>Data encryption</td>
</tr>
<tr>
<td></td>
<td>Interoperability</td>
<td></td>
</tr>
</tbody>
</table>

**Go with CSP?** NO

**Monitoring And Continuous Improvement**
also important because it prevents attacks and intrusion from unauthorized third parties. The widespread use of smartphones and their growing capabilities [33] in modern healthcare requires a solid layer of mobile security [34]. And finally, the CSP needs to demonstrate the level of physical security of the data center where the healthcare data is stored.

The second aspect of Phase I is the need to complete a detailed financial analysis with respect to outsourcing data and/or services to a third party on the cloud. Discovering the needs of potential users (physicians, nurses, lab workers, clinical trial researchers, payroll, upper management, etc.) should be done as well. It is highly possible that the different groups have different needs and expectations. Yet, with many stakeholders involved in the process, it is possible to reach higher levels of user satisfaction, system quality and system use [35, 36]. Cost and Return on investment (ROI) needs to be considered because in some cases it may not be feasible to invest in an off-the-shelf EHR system or maybe the particular vendor may not be the most feasible option. Sometimes there are potential hidden costs that are not included in the initial estimation.

And finally, based on the collected information about the current technical capabilities, the elicited user requirements and the financial analysis, a business decision has to be made. Business continuity should be considered as part of the managerial evaluation process because data availability and interoperability between various healthcare providers are key factors for the CSP selection. Workflow compatibility guarantee seamlessly blend with previous structure without disrupting or changing the existing workflow processes at the healthcare practice. And the last management consideration should be related to the needs of the HR department that may involve access control for users group, the integrity, availability and confidentiality.

3.2 Phase II: Service Level Agreement (SLA)

Before committing to any CSP, the healthcare practice needs to discuss the eventual SLA and to make sure it has its best interests. With respect to compliance with legislation and best business practices, the CSP should be able to demonstrate Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act compliance, since it is essential for the receiving reimbursements according to the American Recovery and Reinvestment Act (ARRA). The usage of Health Level 7 (HL7) standards for messaging is also crucial, as it has become a de facto standard practice for the majority of US medical institutions. There are other Health Information Exchange (HIE) standards which are mandatory for all participating healthcare practices and the need to be reflected in the SLA. Additional certifications and accreditations are highly recommended as they ensure compliance with best practices and demonstrate the CSP’s ability to meet industry standards. The CSP must also present insurance policies in case the data are breached, stolen or accessed by unauthorized parties. This will provide financial guarantees to the healthcare provider and will increase the trust in the CSP. In case of a data breach or a violation, the SLA needs to address these problems and who will be responsible for them. The CSP should also guarantee the sovereignty of data, since the healthcare practice will not have physical access to it most of the time. Thus, it is important to ensure that data will not be compromised or any of their key functions (availability, integrity and confidentiality).

Additionally, data ownership needs to be included in the legal agreement. Ultimately, the customer should be the one to have control of how data is used and accessed and not the CSP. The healthcare practice needs to develop and enforce strict policies on this aspect and the CSP must comply with them. In cases when the customer does not want to use the services of the CSP, the legal contract needs to address the data return process – how long it will take, how it will be organized, who will have access to the data, etc. This is important to consider because the healthcare practice may not be satisfied with the cloud services provided and may want to terminate the contract. Since personal information about patients’ healthcare will be stored on the cloud, it is important to also consider the physical location of the data center. It is recommended to be on US territory in order to avoid the possibility of national security issues related to data breaches, thefts or leakage. Some CSPs also use the data they store for data mining or selling it to other companies for marketing purposes. The legal contract must exclude all such actions as they violate the HIPPA and HITECH Act regulations.

The patients, whose data are going to be stored on the cloud, should be informed about this – how their data are being used, stored, and who will have access to them. Informing the patients and obtaining their written consent is of vital importance for the healthcare practice as this may lead to law suits, financial losses and lack of trust.

3.3 Phase III: Cloud Implementation

Phase III is concerned with the actual implementation of the EHR system on the cloud. First, a pilot implementation should be considered to avoid disrupting the business processes. This will provide an overview of the whole process and will demonstrate the CSP’s ability to organize and support the process. Onsite visits can be helpful to obtain feedback directly from the CSP’s customers and learn from their experience. After successfully completing the monitoring process and being satisfied with the results, the healthcare practice should consider implementing the cloud structure for one system at a time. That way the implementation process will proceed only if the previous system was successfully implemented.

A gradual implementation will allow thorough testing of each module and making sure that there are no bugs and the system functions as expected. The testing process can include stakeholders from various departments. Due to their specific needs, stakeholders may test a number of scenarios and look for specific problems. Integrated EHR systems usually
involve many individuals and processes, thus thorough testing plays an important role in the implementation process. Obtaining stakeholder feedback during the testing can be used not only to fix bugs, but also to suggest future improvements to the system’s capabilities. Stakeholder involvement can also increase user buy-in and improve user satisfaction.

Training is the final step of the implementation process. It needs to be done with all individuals who have access to the data. Data will be shared with many other healthcare providers and it is important to maintain the integrity, authenticity and non-repudiation. Training the users to work with the new system will improve its acceptance and can also help with the proper use of the features and functionalities. Training users, before and after the implementation is complete, increases their skills and knowledge, and helps them to better utilize the capabilities of the system. Obtaining feedback not just from the medical personnel using the cloud solution, but also from the patients is necessary because the ultimate goal of the healthcare services on the cloud is to see improved quality of life for patients and make them more engaged in their own health. A detailed user manual should be provided by the CSP to the healthcare professionals so they can properly utilize the system and refer to it when necessary.

3.4 Phase IV: Evaluation

After implementing the CSP services or model, the next phase is evaluating whether the new system is useful and whether the CSP is delivering the services according to the SLA.

First, certain metrics need to be developed. They may be based on industry benchmarks or documented best practices. Such information is available in technical and medical journals and best practices are shared among the industry professionals. Also, regular security audits with specific criteria will be useful to make sure best practices are being followed.

The evaluation should consider how the system is implementing health standards. For example, the way the CSP deals with HIE in terms of Direct and Connect as means for communication in the National Health Information Network (NHIN); and interoperability between national systems and exchanging data according to the standards approved by the US government.

Evaluation of the existing health standards should be done regularly to reflect changes in legislation regarding application of CSP in healthcare. In addition, user standards regarding best practices in usability, usefulness and technical correction of the data need to be done during the evaluation process to adequately respond to any new improvements or developments in the healthcare cloud security field. And finally, evaluation of the data encryption model should be done because data need to be protected when transferred via the HIE. This is a must and a good way to protect the privacy of patients’ data.

Evaluation from technical perspectives should also consider performance. Speed and capacity of the cloud as well as the frequency of backup are all requirement to maintain validity and reliability of the CSP. Privileges to access should be detailed. Secure multi-tenancy is essential where each customer see only their data and have no access to data belongs to others on the same cloud service [37]. CSP should be able to report logging investigations. Additionally, the portability of data is core criteria in making decision of any CSP to avoid Lock-in.

3.5 Phase V: Monitoring and Continuous Improvement

After implementing the CPS services or model, the final step for the medical practice is to perform continuous monitoring and make improvements to the system.

Making regular audits and searching for new and advanced practices regarding securing health information on the cloud are beneficial for the medical practice. These activities can increase the competitive advantage of the practice and create a sustained superior performance [38]. An assessment exercise can be performed during or after the implementation to identify the success of the project. Different techniques, individually or in combination, can be used to evaluate the implementation. Measuring results against goals, standards, and stated objectives will help managers to evaluate the performance of the project [39]. If the outcome of the evaluation is negative and the CSP fails to provide the necessary services, then looking for a new vendor is highly recommended.

4 Methodology

Our methodology is to use a qualitative survey and interviews to evaluate the proposed framework. The survey will be distributed to medical professionals. Face-to-face interviews with professionals will be conducted. Before that we plan to conduct a pilot test with graduate students and use their feedback to adjust the questions and improve the visual representation of the framework. Cognitive techniques will be used to code the main ideas provided by the respondents in the open-ended questions and interviews. Additionally, a frequency analysis to better understand the background of the respondents will be conducted. The online survey will comprise three sections. The first section informs the participants about the purpose of the study and obtains their consent. The second section contains background information in terms of the healthcare practice and the participants’ level in it. In the third section, the framework is displayed and the participants will be asked to evaluate it based on a five-point Likert scale. Additionally, their feedback using the open-ended questions and interviews will be collected. For this section we used some of the survey questions developed by Motiwalla [40] as they were suitable for obtaining user feedback regarding the usefulness and usability of an artifact.

Since graduate students will complete the pilot survey, they need first to watch a short video online to learn more about
the security issues of EHR on the cloud, as we assumed they had no prior knowledge of the topic. This pilot study aims to make sure questions and explanations are clear enough and the security framework is easy to follow. The survey platform Qualtrics is the tool will be used to store and process the collected data.

Since this is an exploratory study, we plan to collect data from a convenience sample of healthcare professionals and information security experts who would be knowledgeable on the topic and can provide us with valuable feedback and ideas for improving the framework.

5 Discussion

Three possible limitations and recommendations for future research were identified in this study. First, this is an exploratory study on such a broad topic as securing health records on the cloud. We recommend follow-on action design studies to examine the effects of applying the security framework in a real healthcare environment. Specific metrics can be implemented to more accurately evaluate the utility of the proposed artifact. Second, utilizing qualitative techniques and using a case study approach may provide more details on the perspective of healthcare professionals regarding EHR systems on the cloud and the process of vendor selection. And third, the current study can be extended by considering cloud computing opportunities for mobile healthcare (mHealth). Security measures for smartphones are still under development and we recommend others to rely on a classification of knowledge such as the taxonomy of mHealth apps [41] in order to expand the scope of the current study.

6 Conclusion

The goal of this study is to propose a security framework for health records on the cloud. We expect, using the framework, to have a better scientific approach in selecting CSP. The study further demonstrates the effectiveness of having such a comprehensive approach to the decision-making process.

Based on existing literature in healthcare IS, cloud computing and security, we developed a framework and described the methodology to evaluate the proposed artifact.

Our contribution to the existing literature is manifest in several aspects. First, we employ best practices in design science research and apply a design approach to solve an existing problem in healthcare IS. We follow recommendations by [10, 11] to demonstrate utility, usefulness, and the value of the proposed artifact. Second, we review the current state of healthcare information systems, cloud computing, and security to build the foundations of the framework. We summarize best practices and draw upon exemplar studies to provide a high-level concept of the CSP selection process. And third, we provide practical recommendations for improving healthcare IS and achieving the meaningful use criteria. Our artifact is based on prior scientific contributions and demonstrates high relevancy to a growing problem in healthcare IS.

The results of this study also have several implications for practice. By analyzing a medical practice’s needs in terms of securely storing patient data on the cloud, this study provides an understanding of and an insight into the need of thoroughly investigating the CSP proposals in the context of information security. Evidence of the framework’s application and usefulness highlight the importance and consequence of implementing such a tool in medical practices to improve their organizational processes. Healthcare professionals should focus on the security aspects to better protect health records on the cloud. By using the proposed framework, managers can make a more informed decision and select the vendor that can provide most capabilities at a reasonable price. That way, the medical practice can improve its performance, demonstrate meaningful use, and provide better quality of life for its patients.

7 References


