DOI: https://doi.org/10.48009/2_iis_2021_74-83

IT leadership's role in implementing cloud environments for securing clinical data

Angela Munoz, *Middle Georgia State University, angela.munoz@mga.edu*
Michael Ferig, *Middle Georgia State University, michael.ferig@mga.edu*
Pamela Vantine, *Middle Georgia State University, pamela.vantine@mga.edu*

Abstract

The purpose of this paper is to develop an understanding of the role of IT leadership in designing and implementing strategic measures to prevent privacy and security breaches of clinical data in a cloud computing environment. This is presented via a case scenario of a health company. Based on research from cloud-based storage integration projects and analyses, the company's IT leadership team designed and implemented a cloud-based environment that would successfully merge existing clinical systems with advanced security and privacy boundaries, teleworking capabilities, increased patient privacy protocols, and a streamlined onboarding and offboarding process that is both accessible, yet restrictive.

Keywords: leadership, privacy, security, cloud

Introduction

With the integration of Electronic Health Records (EHRs) into cloud-based environments for health clinics, IT leadership must be prepared for the specific privacy and security challenges associated with merging administrative and clinical information into an accessible cloud environment. Challenges associated with cloud-based clinical data stem from strict privacy requirements such as HIPAA-compliance legislation, privacy protections for clinical and billing patient information, and providing security options for these systems that will ensure accessibility and protection. The purpose of this paper is to develop an understanding of the significant impact that IT leadership plays in designing and implementing strategic measures to prevent privacy and security breaches of clinical data in a cloud computing environment. This is presented as a review of literature through a case study of a fictional company - Baxter Health Clinic, whose IT leadership team developed a cloud computing system that would offer significant improvements to accessibility and security, but their leadership team discovered that without the proper security and administrative measures in place, the data was easily exposed and posed a serious privacy and security liability for the clinic. The problem began with the clinic management team's decision to upgrade their paper filing system. The management goal was to upgrade their files into a cloud-based storage service for improved data accessibility, allowing for teleworking capabilities, and to provide quick and easy medical billing.

In 2016, the HIT Infrascruture.com announced that “HIPAA-compliant cloud tools offer the healthcare industry many benefits including cost savings, remote file sharing, custom applications, and expanded storage, giving organizations the ability to create a dynamic, future-proof infrastructure” (O’Dowd, 2016). In the same year, Baxter Health Clinic rushed to complete the cloud-based storage merger, and within a few months, the Information Technology (IT) leadership team realized that they had not fully grasped the various privacy and security issues that may arise after converting their patient and administrative information completely online. The Clinic’s administration was faced with re-evaluating their use of cloud computing services and was tasked with implementing privacy and security measures to protect their data from the illegal breach of important health, billing, and administrative data found in the cloud.

This paper is organized consistent with its purpose. First, a review of the pertinent literature will be presented. Second, there will be an organized analysis of the review of the literature presented that will include a description of the challenges and solutions to be achieved related to privacy and security breaches of clinical data in cloud environments. Next, strategic IT leadership principles and practices will be discussed that directly impact the successful implementation of cloud environments for clinical data. Finally, a concise conclusion to our research will complete this paper.

Review of the literature

The concept of cloud computing was originally designed to assist healthcare facilities with storing multitudes of data since storing vast amounts of data was extremely expensive to store on physical servers. Cloud-based storage has become a growing need for healthcare industries, and the strength of the cloud-based system is heavily reliant on the time, effort, and planning that must be completed by IT leadership. This strategic planning phase is integral for an organization, and it can directly impact the successful implementation of the cloud-based storage system. Also, healthcare industries as well as clinics, are finding that the specific design and implementation associated with integrating a public cloud computing system as a remote storage solution provides a great deal of service agility and boasts significant cost savings for healthcare finances. Though cloud storage offers many advantages, there are also several risks associated with cloud computing technologies such as learning to use a new interface associated with managing a cloud database, managing the encryption key, and preventing abuse and security breaches. Various scholars have offered their respective views and insights into these healthcare data challenges associated with cloud computing services. Because healthcare organizations must also comply with HIPAA compliance legislation, security concerns, and data breaches, Information Technology (IT) leaders must remain vigilant in their pursuit of ethical, professional, and technological solutions (Stantchev, Colomo-Palacios, & Niedermayer, 2014).

The literature regarding security challenges in healthcare cloud computing, in general, concludes that clinical data that is stored by various healthcare organizations is quite sensitive and should not be made readily available or accessible to unauthorized individuals (Mehraeen et al., 2017). Such personal patient information should also be kept private, confidential, and secure so that the sanctity and security of this information would not become compromised by public access. Though with the rapid progression of these types of easily accessible technologies in this dynamic world, cloud computing is still considered vulnerable to cyber security gaps, and this can have a detrimental effect on the confidentiality and safety of patients' electronic healthcare records, and in these cases, IT leadership must quickly recognize and address the specific security issues found within these compromised wireless networks. Recently, security concerns in the cloud computing environment have become increasingly important issues for IT leadership. The review of articles has indicated that it is necessary to provide authentication, authorization, and access controls inside the virtualized cloud network to ensure the continued protection of precious healthcare data. Issues like Identity Protection and Access Control, Internet-based Access, Security and Authorization as well as Cyber-Criminals are primary problems in the area of clinical cloud computing. To better handle these problems, many of the specific processes involved, such as Hybrid Execution Model, Identity Management, VCC-SSF, Hype Hypervisor Security Architecture, as well as Resource Isolation approaches, need to be specified for the use of cloud computing vulnerability management processes (Mehraeen et al., 2017).

In an article by Kuo (2011), it was identified that cloud computing is a modern approach to provide helpful computing tools and facilities. Many administrators and analysts agree that cloud data storage for clinical practices will enhance patient care, benefit the practice of health sciences, and transform the face of health information technology. However, as with any innovation, cloud computing should be rigorously tested by IT professionals before its universal implementation. Healthcare, like any other sector process, involves continual and systemic improvement to remain cost-effective, efficient, as well as to deliver high-quality services. Probably the greatest opposition to cloud storage in health IT centers includes data protection and legal problems. Fortunately, several big providers such as Microsoft, Google, and Amazon, are committed to implementing the best policy and practices to protect user data and privacy. Some non-profit organizations, such as the Cloud Protection Partnership, the Trusted Computing Group, have built detailed standards and hardware and software solutions to help create secure cloud applications. Governments are now interested in promoting legislative regulations (like HIPAA and PIPEDA) to protect data and privacy of cloud users. In comparison, most of the regulatory problems inherent in cloud computing will typically be addressed by contract evaluation or negotiations made by administrative staff. In case certain healthcare organizations are considering the implementation of cloud computing services, it is required that they also allow their IT leadership team to adopt strategic planning methods to closely examine environmental factors such as a feasible budget, the aspect of technologies, culture, staffing, regulations, etc. such that the assessment of these various capabilities can be carefully analyzed, and various strategies can be designed to achieve success (Kuo, 2011).

Soursou (2019) stated that Blockchain technology has attracted significant recognition, with a growing interest in a wide variety of fields, ranging from data storage, financial markets, computer security, IoT, and food sciences to the healthcare and brain research industries. A remarkable interest has been seen in the use of blockchain technologies for the provision of safe and reliable health data storage. In addition, blockchain is transforming existing healthcare procedures to offer a more efficient method of successful diagnosis and treatment through safe and secure data exchange. In the meantime, blockchain might be a tool that could aid in customized, authentic, and safe healthcare by combining all of the patient's real-time clinical data and delivering them in an up-to-date, secure healthcare environment (Soursou, 2019).

Moreover, Kshetri (2013) discussed the challenges of privacy as well as security issues in cloud computing. It was inferred that cloud computing is portrayed in the mainstream press as the next big trend and a significant technical revolution. It is likened and compared to the Industrial Revolution in terms of technical ramifications associated with innovation and economic prosperity. Around the same time, there are major protections and privacy threats involved with the transformational existence of the cloud. There is also a major difference between vendors' statements and consumers' opinions on cloud protection, privacy, and accountability. The response from the cloud industry has been that cloud environments are significantly more secure than previously thought. But several users are still not in support of this claim. Issues such as stability, safety, and availability are among the top considerations of cloud-based decision-making rather than the overall cost of ownership. Therefore, it is required that these issues must be addressed, and safe and protective cloud computing services must be provided to the users (Kshetri, 2013).

According to Chen & Benusa (2017), healthcare is strongly regulated by federal regulations and business guidelines. For instance, The Health Insurance Portability and Accountability Act (HIPAA) is the most important law that changes the healthcare system. HIPAA was enacted as a large congressional effort to overhaul and streamline healthcare practices across the nation. After its introduction, new laws requiring changes to the HIPAA regulations have been passed. Regulatory compliance in the area of medical information technology (InfoSec) and privacy have been named the main problems facing the healthcare sector. However, compliance with HIPAA is not a simple operation. If the healthcare provider has been HIPAA compliant, it must adhere to constant detection and scanning of potential threats and vulnerabilities. Safety is a lead indicator in today's rapidly changing technology world; new threats, as well as vulnerabilities, may emerge when introducing new EHR software, updating to a new operating system, upgrading existing medical equipment, subscribing to cloud computing and related services, or beginning to use a new mobile device for work (Chen & Benusa, 2017).

Terry (2017) suggested that there are still existential challenges for healthcare data protection in the United States and it is inferred that there are growing challenges to the security of health records in the United States. Many federal data protection rules extend only to specific industries, such as healthcare, education, media, and financial services. There are numerous, sectoral alternatives in the absence of robust data security regulations. These privacy laws are substantially limited within their vertical reach, favoring downstream protections like anonymity, authentication, and notice of infringements. The HIPAA regulations have slightly fewer protections than the GDPR but are far broader than the provisions applied to other private industries in the US HIPAA, which provides a comparatively limited scope, effectively referring only to data kept by conventional health providers as well as applying only downstream protections such as confidentiality, security, as well as the notice of infringements. Despite its drawbacks, the HIPAA rules are very comprehensive and usually well enforced. As a result, HIPAA has established standards for patients that all their health details are secure. However, technical innovation and customer preference would almost certainly result in rising volumes of health data being collected and stored beyond the HIPAA-protected region. It is also no wonder that the security of health data in the US faces a risky future that will gradually run contrary to the safeguards provided by our trading partners (Terry, 2017).

Kruse et al. (2016) wrote on the primary focus of big data in healthcare and describes how big data analysis is innovative in many market industries, and healthcare is looking at big data to enable answers to many age-related problems, especially dementia, as well as chronic disease management. Big data would have a major part to play in this transition. Health information systems have enormous ability to improve quality in the delivery of treatment, minimize costs to the health care system, and dramatically enhance patient outcomes. The US government has invested billions of dollars to help the country's healthcare market understand some of these efficiencies and savings. Relevant provisions of the Health Information Technology for Economic and Clinical Health (HITECH) section of the American Recovery and Reinvestment Act recognize the importance of IT in the delivery of healthcare in the United States. The increasing use of technologies is pushing the focus of the healthcare system from disease-centric care to patient-centered care. Big data encourages the appropriate use of evidence-based medicine and allows healthcare professionals to make more educated choices. The literature indicates that a reduction in the cost of computational components, such as storage and encoding, contributes to a reduction in the cost of data-intensive activities (Kruse et al., 2016).

According to Al Ameen et al. (2012), the use of wireless sensor networks (WSN) in healthcare applications is growing at a rapid pace. Numerous applications such as heart rate sensors, blood pressure monitors, and endoscopic capsules are currently in use. A new field known as wireless body area networks (WBAN or simply BAN) has worked to combat the increasing use of sensor technologies in this area. Since most devices and their software are wireless in nature, security and privacy issues are among the main areas of concern. Sensitivity also increases due to the overrated presence of humans. Whether data collected from patients or individuals are accessed with or without the permission of the person due to the need of the device, abuse, or privacy issues still arise. There may also be a risk of significant civil instability due to the concern that such systems may be used to detect and track people by government officials or other private organizations. Proper cooperation between various government departments, academic organizations, and manufacturers is required to resolve these hurdles and ensure smooth implementation. To be properly informed, the public should also be made aware of the advantages and consequences relating to these devices. Rules and regulations such as cyber legislation and current health regulations should be formalized and enforced (Al Ameen et al., 2012).

Analysis and measures taken

After much deliberation and analysis, IT leaders at Baxter Health Clinic determined that a strategic plan should be implemented to allow each area of the clinic including administrative, clinical, and IT teams to complete a full spectrum SWOT analysis to identify and isolate common key strengths, weaknesses, opportunities, and threats involved with using cloud environments for administrative, clinical, and IT data. As a leadership strategy, the IT team discovered that allowing each area of the hospital to meet and complete their SWOT analysis would open a trusted line of communication within each area of the clinic to discuss the beneficial and negative aspects of cloud-based computing that are most pertinent to their line of work and production goals.

Once the SWOT analysis has been completed for each area of the clinic, the IT department would work through each of the key issues and challenges listed to find commonalities between teams. Identifying these commonalities provides a streamlined strategy for tackling the four most important issues and challenges of implementing cloud-based storage within the clinic. For the initial SWOT analysis, the IT leadership team discovered that the prominent strength mentioned was accessibility, the top weakness was security, the leading opportunity was teleworking, and the most common threat was privacy. For this analysis, Baxter Health Clinic will focus on solutions to improve accessibility, security, teleworking capabilities, and protecting privacy in designing and implementing cloud-based environments for clinical and administrative data.

Accessibility

Stantchev et al. (2014) revealed that greater accessibility to healthcare data can be a wonderful asset to a modern clinic, however, it can also lead to compliance issues with HIPAA regulations and can become the dreaded downfall of a cloud-based storage environment. The leading advantages suggested by Stantchev et al. (2014) are that increased accessibility to healthcare data can improve employee and patient satisfaction at a clinic, and can help to reduce duplicate procedures and records, as well as provide efficient and patient-focused care.

The negative aspects of cloud-based storage involve the extensive training required to learn how to safely access and save information to the new storage system, and it requires ethical, legal, and professional training for employees so that they understand the HIPAA compliance legislation required for using cloud environments for clinical and administrative data. From the initial SWOT analysis, our teams determined that accessibility was a strength, but coincidentally it can also become a major weakness for the design and implementation of cloud-based storage of clinical and administrative data when employees are not properly trained with comprehensive onboarding and offboarding practices. IT leadership will therefore incorporate a sophisticated and organized onboarding and offboarding process for new hires and existing employees to improve accessibility for those who require the necessary information and to close accessibility for those who are no longer employed.

Security

For the next area of interest, the IT leadership team at Baxter Health Clinic determined that there were significant weaknesses in the security of clinical and administrative data within the initial layout and functionality of their cloud-based storage system. For instance, Mehraeen et al. (2017) strongly suggest that sensitive protected health information (PHI) often referred to as personal health information, should not be readily accessible to unauthorized individuals, including those within a healthcare clinic who do not have the proper clearance to view such information and do not need to have access to this information to perform their daily duties.

As Mehraeen et al. (2017) recommend providing authentication, authorization, and access controls within the cloud-based storage, IT leadership has determined that a hierarchy of security clearance is needed to maintain a safe and secure cloud network. Based on this analysis all employees at Baxter Health Clinic would require proper authorization clearances to view, access, change, and store information based upon a strategic organization of duties and accessibility requirements. Among these security changes, there may also be Personal Identity Verification (PIV) access cards issued to employees to enter certain buildings, access certain areas, as well as to access information from the cloud. This means that Baxter Health Clinic's cloud-based storage may be organized to allow different levels of security clearance within the cloud-based network and each employee will be notified of their specific security clearance and accessibility limits during their onboarding process. If an employee decides to leave Baxter Health Clinic and seek employment elsewhere, the employee will be given a stringent off-boarding process to return all security access cards and the IT team will reset their passwords and close their account access to the cloud.

Teleworking

One of the most beneficial aspects of using cloud-based storage is having the opportunity to access work files from home, and that is no exception for employees in the healthcare industry such as the employees at Baxter Health Clinic. Teleworking was described as an important strength across the board in the clinic's SWOT analysis since the process relies on modern technology and incorporates the cloud-based storage system to allow employees who have access to certain files to work from home which uses their resources to complete tasks in their home environment and away from the stresses of a busy clinic, and away from the fears of various viruses and colds that are common in a clinical setting. Kuo (2011) suggests that cloud-based data storage for clinical practices enhances patient-focused care with a cost-effective and efficient approach that merges a healthy work-life balance for patients and healthcare employees. While teleworking is considered a strength of Baxter Health Clinic, many employees and patients note that teleworking is overall beneficial since the process allows for employees to continue working when they are unable to travel to work in person, and employees can also meet with their healthcare providers by telehealth visits when those employees are working from home or a remote location.

As with any technology, there are still instances where security and privacy issues come into play, and these must be addressed in the clinical policy for employees and through patient brochures that clearly define privacy rights such as HIPAA, and how the patient can help to prevent privacy and information from being inadvertently disclosed to unwanted individuals. Kuo (2011) discusses how more cloud-based companies are addressing their security and privacy issues related to teleworking by creating their built-in safety and security features to provide the best of accessibility, security, and privacy while teleworking, especially where PPI may be involved. As these systems continue to develop, the IT leadership team at Baxter Health Clinic can continue to make improvements in their system, and as they strategically plan for the future of teleworking within their clinic, they will strive to preserve their teleworking capabilities, while strengthening their cloud-based environment that strongly supports this initiative.

Privacy

The clinical, administrative, and IT teams at Baxter Health Clinic unanimously decided that the most notable threat to their new cloud-based storage network was security. IT leaders were determined to make concerted efforts to tackle this issue at every angle. Kshetri (2013) states that experts working in the field of cloud industries believe that cloud technology is significantly more secure than previously thought. Cloud industry leaders report that most issues with cloud-based storage devices originate from poor planning and organization, internal stability issues, unreported security issues that escalate, and allowing too much-blanketed authority and accessibility (Kshetri, 2013).

Terry (2017) concludes that technical innovations and increased customer preferences will certainly result in increasing volumes of healthcare data being collected and stored in cloud-based storage, and the result is that there will be instances where HIPAA compliance does not give specific clarifications. Because of the changing landscape of healthcare data, policies and practices will likely change just as quickly. IT leadership is destined to face a risky and uncertain future that can further de-rail even carefully planned security measures.

For this reason, it will be detrimental for IT leaders at Baxter Health Clinic to foster relationships with technology leaders in the use of cloud-based data storage, but also to proactively initiate relationships with political leaders to become actively involved in healthcare legislation that may hinder technological progress. Kruse et al. (2016) suggest that the increase in cloud-based storage for clinical and administrative data will continue to shape the political landscape for the healthcare industry. These demonstrated efforts to improve health and protect data will be led by IT leaders whose focus will be patient-centered care instead of disease-centric care. Big data analytics will become increasingly more involved in the processes and procedures taking place at even small clinics, and as IT teams to assist in collecting data that will be available in the cloud, patients will have more detailed and concise information about their health choices and preferences.

Conclusion

Cloud computing environments are shown to significantly impact how IT leadership designs and implements strategic measures to prevent privacy and security breaches with clinical and administrative data. With cloud computing, clinics such as the Baxter Health Clinic have many options with accessibility, flexibility, and the ability to comply with necessary HIPAA regulations and therefore, these decisions need to be carefully planned and tested before complete implementation.

In the review of this case study, Baxter Health Clinic implemented cloud-based storage to offer greater accessibility to improve employee and patient care. Healthcare employees could access a patient file easily even while visiting another clinic or doctor’s office, giving improved and more efficient access to patient healthcare records. With patient files easily and quickly accessible, the patient can seek proper treatments quickly and the patient will spend considerably less time at the clinic. However, having this type of streamlined accessibility requires extensive training and exceptional organization on behalf of IT leadership to maintain required HIPAA regulations and design an easily navigational framework for users.

The IT leadership team initially noticed specific security issues within the cloud-based storage network that did not meet the requirements needed for patient privacy, and they were tasked with addressing each issue to create a unique solution. This is when authentication, authorization, and access controls to the cloud-based storage were implemented by IT leadership. Along with the access controls to retrieve and view the information in the cloud, access controls were implemented in certain parts of the building, as well as in certain restricted areas to prevent unauthorized individuals from accessing secured locations and private documents that must be available in physical form. Overall, the more streamlined onboarding and offboarding process were beneficial for new hires, as well as retiring employees, as they were held accountable and responsible for their accessibility choices.

The cloud-based storage also allowed for teleworking capabilities for healthcare providers that ultimately enhanced patient-focused care. Teleworking agreements and scheduling became very cost-effective and gave a great work-life balance for the workers, as well as offering options for patients such as telehealth visits. This gave employees the added ability to work with flexibility in their daily schedules and to travel while accessing all of their routine files and software online. Due to the nature of accessibility, this also created an opportunity for employees to save on gas money, continue to work while unable to enter the office and create a greater need for technological improvements within the clinic. IT leadership saw that this was a notable opportunity in all areas of the clinic, and they created a structural framework to support the growth of this initiative.

Cloud-based storage benefited Baxter Health Clinic in various aspects, by allowing information to become readily available for staff, creating security and privacy boundaries, offering teleworking capabilities, and increasing privacy. With each new opportunity came another possible challenge that needed to be resolved, and this led to the creation of an official onboarding and offboarding process, restrictions, and streamlined user accounts with security access requirements. Accessibility was a challenge and an opportunity in one, since the adoption of this new technology was appealing, but also tricky to ensure that all HIPAA regulations were also being met with great care. Accessibility has finally become a positive addition to Baxter Clinic through the use of cloud-based storage, however additional training was enacted to address improved security and privacy measures and will continue to guide the future of IT leadership involvement and initiatives for Baxter Health Clinic.

In summary, IT leaders can further develop these strategies to focus on addressing specific cloud-based storage challenges such as HIPAA compliance legislation within an integrated on-site and cloud-based health clinic, and how to improve relationships within the clinic through training, onboarding, and offboarding programs, as well as teleworking initiatives. The data and research included in this paper should provide a basic outline for those challenges and solutions that can be imposed to prepare IT leaders for the challenges and vulnerabilities that lie ahead while merging systems. Standardized methodologies could be designed to provide IT leaders with the framework necessary to build strong cloud environments with a specific focus on resolving challenges and building initiatives for advancement within these cloud-based storage solutions. Health practitioners will play a critical role in the future of cloud usage within health clinics, as the system heavily relies on their participation, level of training, and dedication to the integration initiative. Patients will likewise benefit from the many accessibility options such as accessing health records, telehealth capabilities, and real-time updates on their clinical tests and treatment options. IT leadership will continue to lead in innovative practices as they provide further research and data for addressing key challenges and strive to protect important accessibility opportunities that are commonalities between health clinics as they technologically merge into cloud-based environments.

References

Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems*, *36*(1), 93-101.

Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management*, *10*(2), 135-146.

Kruse, C. S., Goswamy, R., Raval, Y. J., & Marawi, S. (2016). Challenges and opportunities of big data in healthcare: a systematic review. *JMIR medical informatics*, *4*(4), e38.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, *37*(4-5), 372-386.

Kuo, M. H. (2011). Opportunities and challenges of cloud computing to improve health care services. *Journal of medical Internet research*, *13*(3), e67.

Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2017). Security challenges in healthcare cloud computing: a systematic review. *Global Journal of Health Science*, *9*(3), 157-157.

O'Dowd, E. (2016, November 29). Understanding HIPAA-compliant cloud options for health IT. Retrieved February 06, 2021, from https://hitinfrastructure.com/features/understanding-hipaa-compliant-cloud-options-for-health-it

Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography*, *3*(1), 3.

Stantchev, V., Colomo-Palacios, R., & Niedermayer, M. (2014). Cloud computing based systems for healthcare.

Terry, N. (2017). Existential challenges for healthcare data protection in the United States. *Ethics, Medicine and Public Health*, *3*(1), 19-27.