Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2019, 6(7):67-70

Research Article ISSN: 2394 - 658X

Data Privacy and Security concerns in Cloud based Health care information systems

Swapna Nadakuditi

Adv IT Business Systems Analyst Florida Blue

ABSTRACT

The healthcare industry is one of the most data intensive industries. Due to increased data volumes, the need to have well-structured information systems to manage and store the data and the electronic system to retrieve the information becomes a critical need for this industry. Electronic Medical Record (EMR) is a powerful tool and provides a multitude of benefits that many hospitals today are considering accepting and adopting this technology to provide medical information and healthcare services in a better way. With the help of large data warehouses that house clinical information, the EMRs help clinicians significantly enhance the quality of medical care and increase the efficiency of medical practice. However, the cost associated with hosting and storing the ever-growing clinical data is putting a huge burden on the healthcare industry both in terms of skilled personnel to maintain the on-prem solutions and the need for advanced hardware setup. Hence there is an increased demand for cloud-based solutions that could mitigate some of these impacts and we are seeing an exponential growth in the health care organizations adopting these cloud solutions.

Key words: Cloud, On-Prem, EMR, Meaningful use, privacy, security, cyberattacks.

INTRODUCTION

The growth of Cloud technology in healthcare resulted in new software tools to help with providing faster patient care with better outcomes and information sharing across systems and organizations and reducing the cost of care. Cloud based solutions can offset many limitations on hosting the data in physical servers and there by providing the organizations with scalability, cost efficiency, disaster recovery, accessibility, advanced analytics, and agility thereby increasing the adoption of these solutions at a rapid pace.

Due to the government's push for meaningful use, healthcare organizations' adoption of cloud-based information systems has significantly increased in the last few years without any focus on implementing adequate security controls Patient Privacy and confidentiality continue to be the biggest issues with modern healthcare systems where the data is easily accessible by everyone. Increased risk of cyberattacks, including data breaches and various kinds of malware resulted due to the heavy dependence of technology. Growing healthcare costs, lack of global healthcare regulations, shortage of skilled work force and resources are some more issues in the current day.

The data privacy and security concerns in healthcare are predominant due to the sensitive nature of the member ePHI. This article aims to review some of these privacy and security concerns when it comes to cloud solutions and the strategies the organizations can apply to mitigate some of these concerns.

WHAT IS CLOUD BASED HEALTH CARE INFORMATION SYSTEMS?

A cloud is a network of remote servers or systems which stores and process data and can be accessed from anywhere across the globe through the internet.

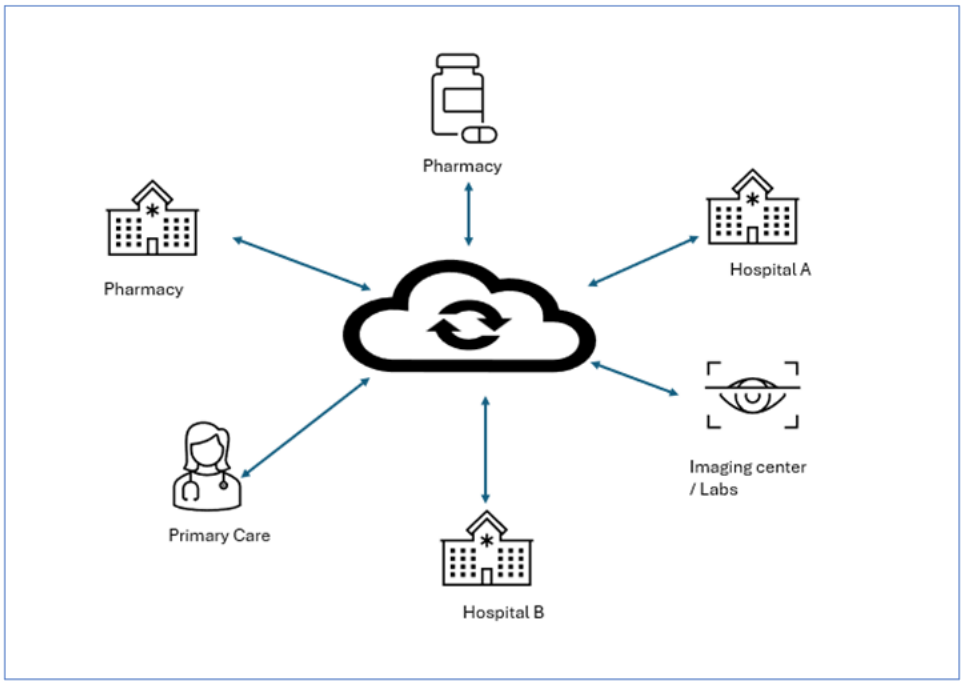

Figure 1: An example of cloud-based health information system

Cloud based health care information systems are used by the health care organizations for storing both clinical and non-clinical patient information such as patient PHI information, their other health conditions, lab results and clinical notes. This helps with easy maintenance and accessing the data by the multi-disciplinary health care teams. These cloud solutions can connect to other health care systems such as EHR using the application programming interface (API). These APIs can connect to different systems and bring the data together into one central location. A third-party cloud provider manages the cloud solutions thus relieving the burden for the healthcare organizations.

DATA PRIVACY AND SECURITY CONCERNS IN CLOUD-BASED HEALTHCARE INFORMATION SYSTEMS

While cloud technology has been beneficial by enabling healthcare organizations with data availability and aid in decision making, there is a need to protect the patient information from being used for unauthorized purposes. Cloud infrastructure comes with challenges in storing patient records in a cloud-based centralized database and these systems are prone to errors, attacks, and data loss due to a single point of failure. Cloud-based systems also face the issues of system vulnerability, data fragmentation, lack of accountability, security, and privacy. Hence information security in health care is especially important not only for the patients but also for the success of any health care organization because the consequences of inappropriate access to healthcare data, loss of data can be multifold.

Here are some key considerations pertaining to data privacy and security concerns exist in the cloud-based health information systems.

Data Breaches: The cloud-based information systems are vulnerable to unauthorized access to sensitive information in the form of cyberattacks. This is due to inadequate security controls in the cloud solutions used in the organization. According to the US Department of Health and Human Services Office for Civil Rights' Breach Portal, there were more than 325,000 healthcare data breaches that were reported until February of 2017.While it is not possible to predict an attack, there are multiple ways to prevent these attacks from happening. According to the IBM Security Services Cyber Security Intelligence Index, more than 95% of these attacks are caused due to "human error" where the users mistakenly access or click on malicious links or web pages [1].

Compliance and Regulatory Requirements: The HIPAA Security Rule mandates the healthcare players to protect the patients' information stored electronically (known as ePHI) ensuring confidentiality, integrity, and security with the help of administrative, physical, and technical safeguards [2].In United states, the healthcare

organizations must be compliant with the HIPAA regulations by ensuring there are adequate security measures in place while storing patient information in the cloud. Whereas the HIPAA privacy rule protects the privacy and disclosure of the health information including the health records and the insurance details of the member. In Europe, the General Data Protection Regulation (GDPR) framework ensures that there are set for information collected from individuals who reside in European union and outside thus enabling the individual's control over their own data than the organizations collecting the information, and this is applicable irrespective of the location of where the cloud data is hosted. By ensuring the data is stored in accordance with the regulations of the country in which the cloud server is hosted will also help mitigate the compliance and legal issues.

Data Encryption: Unprotected data be it at rest or in transit can be highly susceptible to attacks such as interception, tampering, or ransomware and hence need protection in both stages. Data in rest refers to the inactive data that is currently stored in systems without any movement from one network to another whereas the data in transit is the actively moving data from one network to another. While data at rest is less prone to unauthorized access than the transit state, ensuring adequate network controls and stronger encryption algorithms on the data would prevent unauthorized access at cluster or at the storage system and determine the risk profile in both stages. The Secure Sockets Layer/Transport Layer Security (SSL/TLS) is the most popular protocol for data-in-transit which is used to create a secure connection between the two systems that are transmitting data and encrypts the data transmitted. The cryptographic algorithms are used to encrypt data at rest which will convert the stored data into cipher text that can be later decrypted using some keys.

Access Controls: The cloud-based health care systems can be accessed in the network via various clients like laptop phones etc. thus raising a risk for distributed denial of service (DDOS) attacks on the system. Therefore, it is important to enforce strict access controls in the form of role-based security or multifactor authentication so that only authorized individuals would be able to login and access the sensitive patient information. Periodic audits on these access controls would mitigate unauthorized access to the system.

Data Loss Prevention: Data loss prevention is a mix of people, technology and processes that work together to prevent loss of sensitive data. The DLP helps achieve the HIPAA and GDPR regulatory requirements by monitoring and preventing any unsafe data transmission and use of sensitive data in the cloud systems. It helps safeguard data by ensuring controls such as data backups, data governance, data encryption and access restrictions are in place thus making it possible to counter the attacks. For instance, Methodist Hospitals were able to restore the data from backups, a minimum requirement to have when one is dealing with critical patient information. The incident with the Kentuckian Hospital is a notable example of how ransoms can be avoided if officials think quickly and smartly, saving money and life-saving details about their patients [3].

Cloud Service Provider: When planning to migrate to cloud services and selecting the cloud service provider, it is important to understand the security standards that the CSPs would adhere to. The CSPs are responsible for ensuring that there are adequate controls in place to support the regulatory requirements such as meaningful use by protecting the sensitive data and a detailed disaster recovery plan to mitigate any risks with attacks and data loss. There are multiple third-party cloud service providers in the market such as Microsoft Azure or Google cloud which provide Cloud security as a service in the Cloud infrastructure then alleviating the burden of data security from the healthcare organizations.

Security Monitoring and Incident Response: Failure of setting up proactive incidence response and security monitoring for the cloud systems can have catastrophic impacts to any organization and healthcare is no exception. Incidence response refers to a strategic approach to identify and manage vulnerabilities and cyberattacks thereby minimizing the impacts and downtime of the systems. Security monitoring on the other hand is a process of continuously verifying the network for threats and responding to those threats in real time. Security monitoring is critical to ensure that there are adequate firewalls in place, security patches and anti-virus software are up to date on all the systems on the cloud infrastructure. This would help protect data in the systems and prevent malware from spreading once detected by ensuring there are sufficient backups for the server to recover data and to switch to the backup data server when needed by removing the impacted systems from the network.

Therefore, ensuring that these data privacy and security concerns in the cloud-based healthcare information systems are addressed is critical for healthcare organizations to follow the regulatory requirements and the meaningful use of data. With thorough testing and periodic monitoring of the controls, the organizations can detect any significant vulnerabilities in their systems and have advanced knowledge of any potential risks before

there is extensive damage. With the cloud service providers having full control and access to the data users would be hesitant to share their information. Ensuring strict security measures and providing controls for members secure means to access their data would promote trust and more adoption cloud-based services [4].

CONCLUSION

There is never a one-size-fits-all solution when it comes to choosing a model whether on-prem or cloud that works for health organizations. While there are significant cost savings offered by the cloud solutions that should never be the only reason to do so.

Despite a significant increase in IT utilization in recent years, many healthcare organizations did not implement required network security, and other information technology protocols for data protection and skilled personnel to fight against any potential threats and cloud infrastructure is no exception. Aside from backups, many sources including the FBI and top-level cybersecurity firms publish details on how to prevent breaches and how to get rid of well-known malware. These can be advantageous for anyone in computer-related industries. Being more vigilant about what one is accessing, and to make sure everyone is educated about how harmful ransomware can be, although the medical sector should take heed due to their necessity. With proper focus on disaster recovery and increasing IT footprint to mitigate the threats, healthcare organizations not only will be able to prevent any attacks from happening but also reduce costs associated in getting the organization up and running and protecting the organization's reputation.

REFERENCES

[1]. N. Spence, N. Bhardwaj, D. P. Paul Lii and A. Coustasse, "Ransomware in Healthcare Facilities: A Harbinger of the Future?," *Perspectives in health information management / AHIMA, American Health Information Management Association,* 2018.

[2]. "https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis".*American Medical Association (AMA).*

[3]. K. Zetter, "Why Hospitals Are the Perfect Targets for Ransomware," 30 march 2016.

[4]. D. Thilakanathan, R. A. Calvo, S. Chen, S. Nepal and G. Nick, "Facilitating Secure Sharing of Personal Health Data in the Cloud," *JMIR Med Inform,* 2016.