*Journal of Cyber Security*
DOI: 10.32604/jcs.2022.035446

***Article***

Tech Science Press

# Cybersecurity Plan for a Healthcare Cloud-Based Solutions

**A. S. Yusuf[1,*] and A. Q. Ayinde[2]**

[1]New York Institute of Technology, Old Westbury, NY, 11568, USA
[2]Northcentral University, Scottsdale, AZ, 85255, USA
*Corresponding Author: A. S. Yusuf. Email: coloabiodun@gmail.com

Received: 01 September 2022; Accepted: 02 September 2022

**Abstract:** Hospitals provide daily health services for thousands of patients. People, processes, and technologies drive the objectives and goals of the hospitals to ensure optimal and satisfactory health care services are rendered to their customers. Due to the sensitivity of the organization data and patient data, it is essential to ensure that the confidentiality, integrity, availability, and security of these data are considered. The leadership of the organization (managers and executives) must integrate a robust security plan when choosing the technologies that will be used to drive the organization's processes. This paper will evaluate the existing technologies risk assessment, and the importance of adopting new technologies will be discussed. Security plans will be integrated for inventoried technologies and the latest technologies to be adopted while assessing the risk assessment and providing mitigation plans for the technologies.

**Keywords:** Risk assessment; healthcare; cybersecurity; patient

## 1 Introduction

Hospital network infrastructure consists of assets (hardware and software), people, and processes. The policies and industry standards need to be implemented across the hospital network to ensure that organization governance is enforced to prevent any incident of vulnerabilities or mitigate risks or threats. The security operation centers of the organization need to update, monitor, inspect, upgrade, patch, and discard any asset that is susceptible to vulnerabilities. For a proper risk assessment plan, the list of inventories must be monitored and tracked in real-time. Over the years, the data storage has predominantly been on-premises and with the growth in data virtualization, it is important that hospital should move its storage to cloud. Based on the literature reviewed, application managers need to document the vulnerability level for applications, systems, processes and practices that are used for business operation. EHS is one of the new technologies most organization have adopted to drive their clinical-technical business processes related to patient care and services. Electronic Health Systems (EHS) contains Patient MyChart used by the patient for payment and scheduling appointments (in-person and virtual), EHS used by clinicians to process, document, and analyze patient data for hospital consumption, EHS databases are used by analysts to build a real-time dashboard, crystal reports and reporting applications that can be used for appropriate decision making by managers and executives across the healthcare industry to improve the quality of health care services. Despite the vast functionalities of the EHS, there are emergent worries that cybersecurity within healthcare is not robust and has led to a lack of confidentiality and availability [1] and integrity and security of electronic health records [2].

## 2 Technology Reviews and Analysis

Since the adoption of the electronic health technologies by hospital to drive their business, the organization's business operations have been scaled by 400 percent, and the revenue of the organization has grown tremendously due to operation digitalization and network virtualization. The EHS provided a payment platform where patients can pay for their medical bills in the comfort of their homes, Clinicians (Physicians, Nurse Practitioners, and Nurses) can send medication orders to a nearby pharmacy closer to the patient's address. Also, patients can access and print their medical records online with their approved and authorized credentials. The EHS is presently deployed as an on-premises application, leading to its unavailability, inadequate data security, poor data storage and maintenance culture, and poor optimization of the EHS resources.

Data protection is not guaranteed because the IT department manually maintains the on-premises solutions by the employees' productivity server on-premises, backing up data, and maintaining log data will not only reduce the productivity of the employees but is highly expensive as more funds and resources will have to be channeled to the process across the hospital network. This can cause a potential data breach because the process is manual, and the hardware specifications must be reviewed timely as the number of patients being served grows exponentially. Since each dedicated IT associate is attached to each of the on-premises systems at each hospital location, the cost of setting up the hardware, upgrading the hardware, or changing the hardware will not only put excessive work on the employees but also comes with a negative cost implication for the organization [3]. Each location has its own database; merging it into a centralized database will be an additional cost to the organization.

A cloud based EHS must be adopted by most hospitals to ensure that the system's functionalities are optimized and to integrate a robust security plan across the organization. The cloud-based solution will be based on the Software-as-a-service (SaaS) model, which solves most of the problems encountered by the existing on-premises solution deployed for the EHS. The hardware requirements for the cloud-based solution are lower since the software runs on the vendor's (cloud provider) hardware. Maintenance and data backup is automated and done by the provider, reducing the workload on the IT department. This solution is cost-friendly and scalable because additional licenses can be other as the number of users within the organization grows.

It is essential to understand the setback that comes with the adoption of a cloud-based solution for the EHS before it is deployed across the organization. The risk assessment plan must be evaluated, and mitigation strategies must be in place after the cloud-based solution has been adopted or the existing infrastructure will be migrated to the cloud service. During the assessment process, the data breach, insecure interfaces, denial of service, user account compromise, and cloud misconfiguration were identified as the potential risk or threats to the cloud-based service to be adopted.

EHS data breaches can either be internal (within the organization) or external when an attacker uses ransomware via a link to gain access to the organization's sensitive data or via other means to take advantage of the system's vulnerability. A security plan that will enforce industry standards, policies, and processes that tore that both organization and customer data are protected and prevented from getting into the hands of unauthorized users must be adopted. A credential authentication technology must be deployed to monitor the user's logging activities automatically. Users will be registered within the system and, roles will be assigned to prevent who has access to the EHS. Password security questions will be set up within the system during the user (patient or clinician) registration phase, this process will prevent account hijacking by hackers.

Inbound and Outbound ports must be restricted to avoid cloud misconfiguration. To prevent attackers from sniffing the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) ports it is vital to track all the open ports to create security events like data exfiltration and scanning of the entire network whenever the EHS is compromised. Outbound access should permanently be restricted to Secure Shell (SSH) or Remote Desktop Protocol (RDP), a cloud misconfiguration example. Less privilege principle must be adopted to prevent unwarranted use of open ports for SSH. Understandably, an insecure cloud-based solution will expose the EHS to threats. The organization needs to conduct oversight to evaluate the API vulnerabilities on or before adoption. The API should provide relevant feedback whenever the API is us. Should an incident occur, the API must notify the monitoring team so that the incident can be contained and fixed immediately, preventing unwanted exposure to the organization's sensitive data.

The cloud-based environment is experiencing an increase in denial-of-service (DDoS) attacks, one of the most wrecking cyber-attacks. The cloud service provider must provide adequate security solutions for the organization to prevent attackers from targeting the organization domain in the cloud, which may result in a traffic bottleneck when the traffic across the network increases geometrically within a short period. These attacks may cause the EHS servers and the network devices powering the system to shut down. Since most of the EHS will be virtualized, it will make the system susceptible to attackers because it requires securing the extra layer [4]. The security of the virtual machine powering the EHS is essential to prevent unavailability or data breaches should the machine is attacked by the attackers. Instance learning classifiers can be applied in training and testing the virtual machine when analyzing the data to detect the patterns or trends of attacks and predict future threats using the data coming from the EHS system [5,6]. The virtualized environment is highly vulnerable when the virtual machine monitor is isolated and compromised.

## 3 Conclusion

The network security team must understand that malware is a significant threat to cloud-based solutions, primarily when the client-side and endpoint security software has been implemented. The network security team needs to implement-layer security to detect and prevent malware. This double-layer security will contain the malware in the cloud from spreading quickly in the EHS that has been infiltrated. If the malware is not immediately detected, it will weaken the system and cause a severe attack. The vendor must provide the cloud infrastructural services to protect the cloud infrastructure attack.

To ensure that cloud infrastructure is fully secured, the network monitoring team must block all access to confirm the system using least privilege and multi-factor authentication. Network segmentation must be enforced and mandated across the network because should an incident occurs, only a small segment will be affected in the EHS.

**Funding statement:** The authors received no specific funding for this study.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] D. V. Dimitrov, “Medical internet of things and big data in healthcare,” *International Journal of E-Health and Medical Communications*, vol. 22, pp. 156–163, 2016. References-Scientific Research Publishing.

[2] T. Walker, “Interoperability a must for hospitals, but it comes with risks,” 2017. [Online]. Available: https://www.managedhealthcareexecutive.com/view/interoperability-must-hospitals-it-comes-risks.

[3] S. I. Bairagi and A. O. Bang, “Cloud computing: History, architecture, security issues,” *International Journal of Advent Research in Computer and Electronics*, 2015. https://www.researchgate.net/publication/323967455_Cloud_Computing_History_Architecture_Security_Issues.

[4] D. Owens, “Securing elasticity in the cloud,” 2010. [Online]. Available: https://www.sciepub.com/reference/144783.

[5] N. Urenna, A. Abiodun and O. Yemisi, “Application of instance learning algorithms to analyze logistics data,” *International Journal of Engineering Research & Technology (IJERT)*, vol. 10, no. 7, pp. 11–12, 2021.

[6] N. Urenna, A. Abiodun, K. Isolagbenla and A. Yusuf, “Pattern mining of hospitalization data of COVID-19 patients with underlying conditions,” *International Journal of Engineering Research & Technology (IJERT)*, vol. 11, no. 5, pp. 131, 2022.