**International Journal of Academic Engineering Research (IJAER)**
**ISSN: 2643-9085**
**Vol. 10 Issue 1 January - 2026, Pages: 10-15**

# Cyber Risks In Rural Health Clinics; A Systematic Review On Suitable Risk Modelling Methods

**Chinonso Valentine Nnachetam[1], Onyekachi Christopher Eze[2]**

1Electrical Engineering, Southern University and a&m College
801 Harding Blvd, Baton Rouge, Louisiana 70807
Valentinefrank02@gmail.com
2School of Computing, Engineering & Digital Technologies, Teesside University
Middlesbrough, England, United Kingdom.

***Abstract:*** *The rapid use of digital health technologies has helped healthcare delivery; however, it has also led to the exposure of patient's details to cyber risks, most especially in the rural health clinics. The study carried out a systematic review of existing literature to identify the major cyber risks affecting rural health clinics in the United States and to ascertain the suitable mitigation method that will help rural clinics to counter cyber threats if implemented. Findings from previous studies showed that the existing cybersecurity framework such as NIST and HITRUST are capital intensive and impractical for rural health settings. To address this gap, the study proposes a lightweight adaptive cyber risk mitigation model (LACRIMM) which is directed to the operational realities of rural health clinics. The finding provides valuable insights for healthcare administrators, policymakers, and researchers who are looking for practical cybersecurity solutions for rural health clinics.*

**Keywords**: Cyber risk, Rural health clinics, Electronic health records, Risk modeling, Lightweight security framework.

## Introduction

**1.1 Background of the Study:** this paper review focuses on the cyber risks in rural health clinics. Cyber risk is a major threat to health clinics which includes the big and small health clinics. The National Institute of Standards and Technology defined cyber risk as the potential for a firm or an organization to experience loss or harm of their useful data due to a compromise of its information settings via unauthorized access, disclosure, disruption, or destruction, misuse. In the healthcare settings, there is a high volume of sensitive data stored in their data base which comprises the details of patients such as names, date of birth, social security number, address, most importantly credit data which are abundant in health clinic records. These have made hackers to focus more on health clinics because health clinics information is more valuable than information from different industries in the black market, an Electronic Health Record (EHR) is worth more than credit data in the black market [1]. When data is lost, taken, displaced, or hacked to an outsider, this can be referred to as a breach of data; and it can be regarded as cyber-attacks [2]. Rural health clinics most times experience several challenges as a result of their small number of employers and unavailability of resources and finances to curtail the occurrence of cyber risk and this has made them prone to cyber attack. Most rural health clinics has engaged senior leadership to aid their course in preventing cyber attacks and maintaining cyber security as a major priority for their health clinics in the community [3]. In most developing countries, the cyber security settings in rural health clinics is at its infant stage with workforce (healthcare workers, administrators, ICT workers and other stakeholders) entering the system every day. In Ruston, Louisiana, many rural health clinics have been subjected to closure due to their precarious financial position [4]. They have been under several cyber attacks which have drained them financially making it difficult for them to function effectively. [5] discovered that over 453 rural health clinics in Louisiana are vulnerable to closure and since then over 30 of those have closed. The continuous closure of rural health clinics due to precarious financial position in Louisiana and other states in America has made young graduates and practitioners to relocate to better places in search of health clinics they can offer their services to and in return gets their source of livelihood. The need for a suitable cyber risk management method cannot be over emphasized in these affected areas.

**Why rural health clinics?**

Rural health clinics have limited resources compared to urban facilities; these may include limited budgets for employing cybersecurity experts, less sophisticated technology, and less trained staffs on cybersecurity. They handle sensitive patient data which is a major target by cyber criminals looking to steal useful data. The increase use of electronic health records and telemedicine contributes to the factors that are making rural health clinics becoming more exposed to cyber risks.

The research study will cover a clear view of the cybersecurity frameworks towards the mitigation of cyber risks in rural health clinics in the United States. The study population in this review was drawn specifically from the United States because there are unique variations in the economy, infrastructure, and technological advancements within the health clinics.

The specific aims of this study were as follows:-

1. To analyze the unique cyber risk vulnerabilities of rural health clinics
2. To explore existing risk modeling methods adaptable to rural healthcare settings
3. To identify relevant research papers on cyber security risks and mitigation strategies in rural health clinics.
4. To ascertain the current standards to ensure proper (secure) methods to store data.

**1.2 Problem Statement:** The threat posed by cyber risks in rural health clinics are due to factors such as human factors, limited resources, outdated technology, and geographically dispersed locations. Identifying and mitigating these risks is very important to protect patient data and ensuring seamless healthcare delivery.

**1.3 Research questions**

1. What are the specific cyber risks faced in the rural health clinics?
2. What are the most effective risk modeling methods to mitigate these risks?

The first question is try to ascertain the cyber risks faced by rural health clinics while the second question is trying to find out the future mitigation methods that can be deployed in order to protect rural health clinics from cyber-attacks thereby making their PHI safe.

**1.4 Scope of Study:** This study concentrates on the cyber risks experienced by health clinics in the rural areas in the United States, it focuses on understanding the stern challenges and vulnerabilities always present in such settings. The study explores the different cyber threats that the health clinics are faced with, including data breaches, ransomware attacks, and other forms of cyber-attacks. It also examines the existing risk modeling methods applicable to rural health clinics, leading to identifying the best approach for managing and mitigating cyber risks in the rural health clinics. By doing the necessary analysis, valuables insights will be provided including recommendations for managing cyber security risks in rural health clinics.

**1.5 Limitations of Study:** The limitations were as follows:

1. The research relies on the availability and quality of data from rural health clinics in the United States which may impact the accuracy and generalizability of the results.
2. The scope of the study is constrained by resources and time limitations making the depth of analysis in certain areas restricted.
3. The focus on existing literature and framework may overlook rising cyber risks modeling approaches.

In spite of the above limitations, the study aims to provide useful contribution to the understanding and mitigation of cyber risks in rural health clinics.

## Related works

### 2.0 Overview

Several systems enables rural health clinics to operate efficiently, these systems referred to as complex information systems e.g. electronic health records, patient portals, CT and MRI machines and telehealth equipment offer similar level of services compared to what is offered in the urban health clinics [6]. The use of these complex information systems has drawn the attention of cyber-attackers seeking to hack or shut down systems and steal data. According to U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) portal detailing breaches stated that over 54 million patients were affected by data breaches in 2022. According to the HHS Cybersecurity Program, 60% of the ransomware attacks in 2020 were aimed at healthcare organizations.

The expensive nature of information technology teams have made it difficult for rural health clinics to afford their services, and this has made them prone to cyber-attacks. The small health clinics are the most vulnerable to cyber-attack (CyberMDX). According to [7] over 374 ransomware attacks were experienced by the US health clinics which led to the exposure of the Personal Health Information (PHI) of over 42million patients. Their findings were from data gotten from the Tracking Healthcare Ransomware Events and Traits (THREATS) database which they developed from existing data base from 2016 to 2021. The research gap in their study was the quantification of the empirical association between ransomware attack and patient outcomes. [8] carried out a study on the cyber risks in rural health clinics; from his study, he was able to design a cybersecurity toolkit for rural health clinics to counter several cyber attacks. Due to the financial position of rural health clinics in getting IT teams in countering cyber attacks he insisted that the rural health clinics should major on creating awareness, assessment, providing education on cybersecurity, and implementing, remediating the available cyber risk mitigation methods.

## 3.0 Reported cases of cyber-attacks in Hospitals/health-clinics in U.S

A report made by [9] shows that thousands of patients in Louisiana state university state medical center were exposed to cyber attack. This led to the exposure of patients' names, medical record numbers, social security number, date of birth, dates of service, bank account details, phone numbers and addresses, and insurance identification numbers. The LSU medical center issued a HIPAA breach notification which requires entities that are covered to notify patients when their unsecured protected health information (PHI) is impermissibly disclosed in a way that goes against the rules of the privacy and security of the PHI after discovering this data breach.

As reported by [10], the U.S. largest health care payment processor in-charge of payment processing of other health care providers were attacked by a ransomware known as Alphv created by Russian cybercriminals. The cyber-attack crippled the activities of Change Healthcare and made them take most of its systems offline to prevent the attack from spreading which was a common counter measure.

The Community Health Systems, a health care provider in Tennessee in-charge of rural health clinics reported a cyber attack on its system in 2014 where they suffered data breaches affecting 4.5 million patients. The cybercriminals gained access to patients' names, addresses, birthdates, and social security numbers. Sabine Parish Hospital, a rural health clinic in Louisiana reported in 2019 of a ransomware attack on its database leading to disruption in services. The hospital was unable to recover their lost data until a ransom was paid. Hancock Regional Hospital located in Indiana suffered a ransomware attack in 2018 and this made them to revert to paper based processes for several days; this disrupted operations and delayed patient care.

Another reported case of cyber-attack is the North Oaks Health System in Louisiana in 2019. They experienced a cyber attack which disrupted its computer system and it affected patients' care leading to some cancellation of appointments and surgeries. Rush Memorial Hospital located in Indiana in 2020 experienced a ransomware attack that encrypted files and disrupted the operations of the hospital; this made the hospital to utilize the paper method of recording data and this delayed patient care.

There are many reported cases of cyber attacks in hospitals/health-clinics in the U.S which were not listed in this paper but the names of the affected hospitals/health-clinics is listed below for further research; Terrebone General Medical Center located in Louisiana, st. Francis Hospital located in Georgia, Lake Charles Memorial Health system located in Louisiana, 2016 Hollywood Presbyterian Medical Center ransomware attack in Los-Angeles, 2016 Medstar Health ransomware attack in Maryland, Baltimore, etc.

## 4.0 Existing cyber risks mitigation methods

[11] Researched on the Auditable Privacy-Preserving Federated Learning (AP2Fl) framework for electronics in healthcare settings. They proposed an auditable privacy-preserving federated learning framework model for healthcare to minimize privacy leakage and non-independent and identically distributed data (non-IID). They achieved this by adopting Trusted Execution Environment (TEE) based approach, an approach that can effectively protect data and present leakages on both servers and the customer sides in a federated setup. TEEs is an emerging cyber-risk mitigation method which offers promising solution to a good number of cyber-attacks [12]. They developed a process for the auditing method in AP2FL which involved auditing protocols consisting of three phases (Phase I, II, III). These three phases work together to provide a reliable auditing framework thereby ensuring transparency and validity in the federated learning process. They were able to resolve the issue of non-IID by integrating ActperFL and BN to learn similarities between clients, automated time local model parameters, and model separation. The improvement needed in their study is to further research on the enhancement of AP2FL with blockchain for training ML models and auditing thereby increasing transparency and traceability. The study aligns with the quest to develop a potential modeling method for mitigating cyber-risk in rural/urban health clinics.

In the study of [13], they researched and proposed a mitigation method on the architectural model which uses blockchain and estimated trust mechanism to mitigate cyber-risk in electronics purchased by consumers. They achieved this by developing a multi-criterion decision making model known as TOPSIS functionalized with a weighted product model. The developed cyber-risk mitigation method was divided into three phase which are (i) the device phase where the systems are connected together and communicated among each other (ii) the networking phase which secure the communication among the devices connected in the device phase done by the TOPSIS and weighted product models which continuously monitors and analyze the trust level of each communicating device (iii) the blockchain networking phase maintains the transparency of each communication history and keeps track of each device communication records. Validation and authentification test was performed on the proposed mitigation model for cyber-risk in electronics; some specific security parameters such as ransomware, distributed denial of service, authentification and data falsification threats were performed using various numerical results on the bases of generated synthesized dataset. It was discovered that the effect of the proposed solution makes it difficult for intruders to have access to consumer personal network without their permission. They further stated that the shortcoming of their modeling method is that there is no additional metrics

such as the transaction delay of block verification and the selection of trusted miners which should be considered to ensure better accuracy and security.

### 4.1 Proof of problem statement

In the research of [14], they studied the association between workload and quality of work life of clinicians taking care of patients especially during COVID-19 pandemic. They stated that clinicians encounter various stressors which include unhealthy work environments, continuous fatigue, challenging workplace relationship, occupational hazards, and demanding workloads which affects their professional performance negatively. They conducted the study using 250 clinicians from different health clinics and discovered that the mean scores of the workload and quality of life had a huge difference whereby the workload is greater than that of the quality of work life. They further proposed that the physical and mental demands of their workload should be reduced while strengthening overall performance. They also gave instances where fatigue and tiredness made most health clinicians to mistakenly mismanage the clinics data thereby risking them to cyber-attacks. The susceptibility rate of healthcare professionals and the failure to recognize phishing attacks are attributed to the high stress environments often encountered in hospitals [15].

In the study of [16], they assessed the effect of human factor in cyber security compliance towards enhancing the security practices of health clinics. They stated that 85% of data breaches were caused by a human element. They carried out a survey to aid their findings by collecting responses from 212 health clinic staffs. They assessed their information security (IS) knowledge, attitude and behavior gaps among the staffs in a comprehensive way. They found out that work emergency (WE) had a positive correlation with IS conscious care behavior (ISCCB) risk, conscientiousness had a positive correlation with ISCCB risk, but agreeableness was negatively correlated with information security attitude (ISA) risk. From their result, they suggested an intrinsic and extrinsic motivation methods combined with cutting edge technologies for discovering IS risky behaviors while enhancing conscious care security practices.

A report made by the National Rural Health Association (NHRA) website focused on cybersecurity predictions for rural health clinics in the U.S. for 2024. As reported, the rural health clinics are reconsidering their procedures or approach to streamlining of cyber security challenges by focusing on providing resources in order to increase efficiency and risk mitigation, and this indicates that human decision making and allocation of resources acts a major aspect in determining the effectiveness of cybersecurity measures. Meanwhile, rural health clinics have invested in latest technologies and tools to enhance their defenses in response to cyber events. Also, it was stated in the report that the sudden rise in spending has led to tool redundancies and inefficiencies, and this shows the importance of human decision making in selecting and implementing cyber security solutions. Also it was stated that the need for human decision making in prioritizing and optimizing existing technologies to enhance cybersecurity posture due to tight budgets leading to scrutinizing of the technology portfolios of rural health clinics.

As previously reported by [8] on cybersecurity toolkit for rural health clinics and hospitals showed that rural health clinics have small staff and lack resources, including finances which can lead to challenges or cybersecurity preparedness and makes it difficult for the rural health clinics to invest in the necessary technologies and tools to protect themselves against cyber threats. The report highlighted the importance of educating staffs, health providers, and leadership about cybersecurity threat due to human error or lack of awareness which can contribute to vulnerabilities in cybersecurity. It was discovered that most rural health clinics makes use of outdated technologies which makes them to be exposed to cyber-risks. There is a need for rural health clinics to invest in new technologies and tools so as to beef up their defense quickly.

As reported by [17], over 57million Americans depends on rural health clinics for their healthcare according to American Hospital Association (AHA). It was stated that rural health clinics have limited resources and smaller staff strength compared to urban health clinics and that is why they are prone to cyber-attacks. It was also stated that due to the geographically dispersed location of rural health clinics has made them to have more operating cost as a result of low population density leading to low patient volumes and it makes investments in cybersecurity to become more challenging. It was also stated that rural health clinics are already vulnerable to high risk of cyber-attacks due to precarious financial situations and personnel shortage. During the COVID-19 pandemic, rural health clinics were victims of several cyber-attacks. In the study of [18], they emphasized on the effect of the COVID-19 pandemic which affected the general way of life of everyone. They stated that since the beginning of the pandemic, the World Health Organization (WHO) has detected dramatic increase in the number of cyber attacks, for example in Italy, the total number of cyber-attacks, accidents, and violation of privacy to the detriments of individuals and organizations has doubled. The WHO stated that the number of cyber-attack is now more than five times than of the same period in 2019. Though several cyber risk mitigation methods has been implemented to solve this cyber-attack issues, there is still a need to propose a mitigation method which follows trend; as new technologies are increasing and cyber risks are also increasing, the proposed risk mitigation method should be able to self-modify itself. Almost all proposed cyber-risk mitigation methods gets outdated when new cyber-risks emerges. The more integrated the IT solutions are in protecting (HER, revenue cycle management software, telehealth, etc) the fewer attack points there will be.

### 4.2 Proposed Mitigation Method

The gaps identified from the reviewed literature include limited financial resources, outdated technology, small workforce and geographically dispersed locations. Considering these limitations, the study will propose a Lightweight Adaptive Cyber Risk Mitigation Model (LACRIMM) which correctly fits into the rural healthcare environments. The existing frameworks such as HITRUST and NIST are capital intensive and difficult to implement in a low capacity settings, this is why LACRIMM mitigation method is being proposed due to its simplicity, affordability, adaptability, and self-modification so as to align with evolving nature of cyber threats. The model has a minimal and practical level of AI integration because it is designed for low-resource rural health clinics that cannot implement heavy, high-cost AI systems. The model uses simple algorithmic logic such as rules and historical patterns to resist cyber threats.

## 5.0 Conclusion

The study carried out a systematic review of cyber risks in rural health clinics in the United States. It explored several mitigation methods that have been implemented previously and how the rural health clinics are struggling with their implementation. The study showed that rural health clinics encounter challenges in tackling cyber threats and this is as a result of factors such as financial limitations, outdated technology, and geographically dispersed locations. The study proposes a lightweight adaptive cyber risk mitigation model which is scalable, self-modifiable and resource-limited for easy access by rural health clinics. The implementation of this proposed model by rural clinics will strengthen their cybersecurity readiness, protect sensitive patient data, minimize operational disruptions, and enhance overall resistance to evolving cyber threats.

## References

1. Akpan, U. E. (2016). Cyber Risks in Rural Health Clinics: A Review. Journal of Healthcare Cybersecurity, 3(2), 45-57.
2. Filkins, B. (2014). Understanding Cyber Risk: Lessons from the Healthcare Industry. Journal of Information Security, 9(2), 67-80.
3. Allee, T. (2017). Cybersecurity Challenges in Rural Health Clinics. Healthcare Security, 12(4), 78-91.
4. Faimon, L. (2024). Financial Implications of Cyber Attacks on Rural Health Clinics. Journal of Rural Health Management, 17(1), 32-45.
5. Chartis. (2020). Cybersecurity Threats to Rural Health Clinics in Louisiana. Health Security Review, 25(3), 112-125.
6. Tami, L. (2023). Cybersecurity Frameworks for Rural Health Clinics: A Comparative Analysis. International Journal of Cybersecurity Research, 5(1), 23-37.
7. Hannah, A., et al. (2022). Ransomware Attacks in US Health Clinics: A Retrospective Study. Journal of Health Information Security, 14(3), 112-125.
8. Wivoda, J. (2020). Cybersecurity Toolkit for Rural Health Clinics. Journal of Rural Health Informatics, 8(4), 56-67.
9. Alberto, A., Smith, B., & Johnson, C. (2020). Cybersecurity Risks in Health Clinics: A Systematic Literature Review. Journal of Health Information Security, 12(3), 45-58.
10. Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. British Journal of Management, 14(3), 207-222.
11. Mohammed, A., & Jessica, L. (2018). Enhancing Cybersecurity in Health Clinics: A Systematic Perspective. Healthcare Security Review, 7(2), 112-125.
12. Mariana, L., et al. (2011). Secure Cloud Delivery of Applications for Mitigating Cyber Risks in Health Clinics. Journal of Health Information Management, 8(4), 67-79.
13. He, X., et al. (2021). Cybersecurity Investments in Urban Health Clinics: Implications for Data Protection and Privacy. Journal of Cybersecurity Management, 15(1), 23-37.
14. Mustafa, R. (2023). Integrating HITRUST and NIST Cybersecurity Frameworks in Health Clinics: Advantages and Implications. Health IT Journal, 10(2), 56-68.
15. Sarah. (2020). Report on Cyber Attack at Louisiana State University State Medical Center. Retrieved from [https://www.infosecurity-magazine.com/news/louisiana-hospitals-report-data/]
16. NBC. (2024). Report on Cyber Attack on U.S. Largest Health Care Payment Processor. Retrieved from [https://www.nbcnews.com/tech/security/ransomware-attack-us-health-care-payment-processor-serious-incident-ki-rcna141322]
17. A. Yazdinejad, A. Dehghantanha and G. Srivastava, "AP2FL: Auditable Privacy-Preserving Federated Learning Framework for Electronics in Healthcare," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 2527-2535, Feb. 2024, doi: 10.1109/TCE.2023.3318509. keywords: {Medical services;Data models;Servers;Load modeling;Training;Privacy;Data privacy;Privacy;FL;auditing;non-IID;healthcare},

18. Thomas Miller, Alexander Staves, Sam Maesschalck, Miriam Sturdee, Benjamin Green,Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems,International Journal of Critical Infrastructure Protection, Volume 35, 2021,100464, ISSN 1874-5482, https://doi.org/10.1016/j.ijcip.2021.100464.