Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

# Ransomware Attacks on Healthcare Institutions: Vulnerabilities, Impact, and Prevention Strategies: A Review

**Kranthi Kumar Asike Parameshwar**

Department of Technology
Indian Wesleyan University, Middletown, Connecticut, United States.

**Abstract:**
Medical institutions are becoming targets of ransomware attacks, with the attacks increasing between 2016 and 2021, exposing personal health data of almost 42 million patients, and the attacks are becoming larger, with organizations having more than one hospital. Such attacks take advantage of ongoing vulnerabilities like phishing and ageing systems with resulting high disruption levels like patient census of 6114 before the attack to 7039 during attack and recovery in the adjacent emergency departments, long wait time, and high risks to patient safety. Effects go to fiscal losses due to ransom payments executed in the Bitcoin, operational backlogs and psychological stress on employees, with regional spillover effects jeopardizing the provision of acute care. This is a review of weaknesses, effects, and preventive measures, which shows some uniform tendencies of increasing intricacy of attacks, as well as the heightened requirements of interdisciplinary preparedness. It is important to note that since smaller, rural non-profit hospitals have fewer cybersecurity resources, they are disproportionately exposed to risks, and disruption with no ransom payment can be reduced through strategies such as offline backups and training of employees. The evidence highlights a zero-threat environment in which even the single cases can propagate regionally and fill the gap in the consolidated studies of healthcare-specific cyber resilience. It has implications such as policy requirements to federal fund vulnerable institutions, and clinician-based contingency planning to protect patient outcomes, but the measures have gaps in long-term recovery measurements and international comparative data.

**Keywords:** ransomware, healthcare, vulnerabilities, hospitals, phishing, legacy, systems, medical

## 1. Introduction

The healthcare industry is at the centre of the digital revolution, and electronic health records, connected medical devices, and cloud computing services allow achieving unprecedented efficiency in patient care and data management [16, 29]. Nevertheless, this interdependence between information technology has turned hospitals and clinics into ideal prey of cybercriminals, especially through ransomware, a form of malware, which blocks important data and asks to be paid to be unblocked, usually using cryptocurrencies such as Bitcoin [14, 18]. Ransomware attacks have been on the rise in the past few years due to the high price of sensitive patient data, such as personally identifiable information, medical histories, and financial data, that can be sold at a great price in black markets or be used to extort [17, 25]. In a healthcare facility, where even a minute of downtime can pose a direct threat to lives, such an incident derails even emergency triage to regular diagnostics, which can further exacerbate its effects on an organization, not just in monetary terms [22, 32].

The weaknesses that provide opportunities to make such attacks are the combination of technical, human, and systemic factors. Old systems, unpatented software, and phishing through fake emails use vulnerabilities in the cybersecurity infrastructure, and the trend of fast introduction of smart devices and

other IoT integrations is faster than the security patches [1, 24]. Impacts are multi-faceted, and they include immediate operational stoppage, delayed treatments, and consequential effects on regional networks, as experienced in high-profile incidents that resulted in the need to use manual processes and divert ambulances [26, 30]. Although the prevention strategies are diverse, they focus on preventative measures such as training and backups, but their implementation is not universal in institutions [9, 16].

Although there has been an increased awareness, the literature is still scattered with various studies addressing specific cases or trends without integrating the vulnerabilities, effects, and defenses altogether. The gap in the literature is filled by this review with a review of ransomware attacks against healthcare facilities, analyzing the vulnerabilities used to gain access to the facility, the extent of operational and patient-level consequences, and evidence-based prevention and resiliency measures. The combination of qualitative information derived through interviews, cohort studies of disruptions, and the analysis of world events sheds light on this area, a high-stakes field of targeted interventions [2, 29].

## 2. Methods

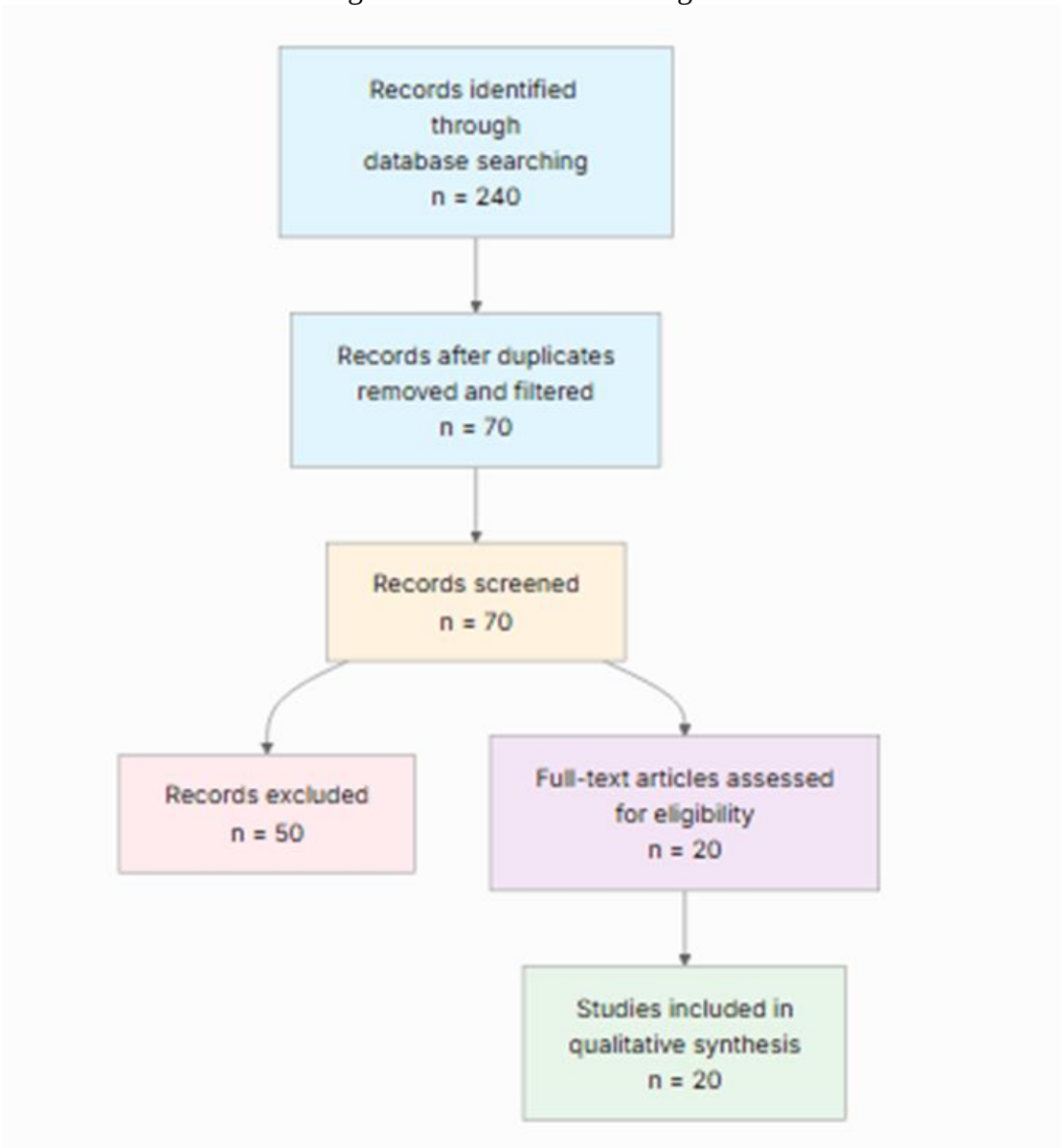
### 2.1 Search Strategy

This research used a broad search in this work to determine the literature on ransomware in healthcare. Two large-scale academic databases (Semantic Scholar and OpenAlex) were searched, as these two academic databases combine and index more than 220 million scholarly publications. The study used a hybrid searching strategy that integrated semantic searching and the use of keywords to guarantee breadth and narrowness of concepts in terms of coverage. The questions were geared to represent different aspects of ransomware in healthcare, such as hospital system vulnerability, phishing, and old medical IT infrastructure; effect on patient care, such as EHR downtime, loss of money, and service outage; and prevention measures like backups, network segmentation, staff training, and best cybersecurity practices. The paper also added questions that focused on case studies of recent large ransomware attacks like WannaCry, Ryuk, and SamSam, literature reviews, and literature surveys on malware encryption and patient data protection. Lastly, questions were expanded to detect recent trends in 2018-2023, such as the ability to do double extortion, Ransomware-as-a-Service (RaaS), and attacks on the supply chain within the health sector. The search process was repeated, and refinements were performed to minimize noise and select the information relevant to the context of healthcare, that is, hospital work, patient safety, and organizational resilience.

### 2.2 Study Selection

Database searching revealed 240 records at the start. The 70 records were filtered by eligibility criteria after duplicate removal and relevancy-based filtering. Out of these, 50 were discarded to give a final synthesis of 20 papers, as shown in **Figure 1**.

Figure 1. PRISMA Flow Diagram




### 2.2.1 Eligibility criteria

The paper particularly focuses on ransomware attacks in healthcare institutions, including hospitals, clinics, and medical institutions, so ransomware attacks and not cyber threats in general are the topic of discussion. It covers the weaknesses that are used in the attacks, such as phishing messages, non-patched or outdated systems, and poor access controls. The effects of ransomware in the healthcare setting are well outlined and include clinical operation and patient care delays, as well as major losses. Moreover, the paper also covers prevention and mitigation measures, including training the staff and updating the system, or incident response plans and data backup. It cites the ransomware attacks and the statistics of 2016, and further confirms they are topical to the current trends in the threat environment. Notably, the paper uses empirical evidence in the form of case studies, surveys, and recorded events in actual healthcare facilities. Lastly, it is written as a review and analysis, and critical points are presented instead of it being a promotional text or a strictly technical implementation manual. All the studies are within the above-mentioned eligibility criteria.

### 2.3 Data Extraction and Synthesis

The paper has various critical weak points of healthcare systems that render them vulnerable to ransomware, such as phishing attacks, use of old systems, lack of updated software patches, poor access controls, and lack of awareness among the employees. Effects on health facilities are devastating, including operational dysfunctions, stalled operations and postponed medical processes, impaired patient care, loss of finances by paying the ransom and recovery expenses, tarnished reputation, and hacking of sensitive patient records. Regarding the prevention measures, the paper focuses on the frequent patching and updates, training of employees on phishing awareness, network segmentation, well-developed backup procedures, incident response planning, and the implementation of sophisticated detection tools. Case studies, including the WannaCry attack on the National Health Service of the United Kingdom that shut down much of the service and the examples with hospitals in the U.S., where patients had their service delayed because of locked systems, are also described in the paper. The article qualifies as a thematic review with a relatively recent publication date, which summarizes the results of several case reports and surveys of ransomware incidents in the medical sector over the last ten years. The general inferences are that ransomware is a longstanding and increasing menace to healthcare, and it has always been demonstrated that healthcare systems with archaic systems and those with low cyber hygiene face the greatest risk of attack. The authors suggest the multi-layered approach to defense, reinforced regulatory frameworks, and intersectoral cooperation as the means of lowering risks. Thematic analysis identified the patterns that occurred repeatedly in studies, and the quality of evidence was regarded as high because it was consistent in many cases that had been documented.

## 3. Results

### 3.1 Characteristics of Included Studies

**Table 1** shows the characteristics of the included studies, covering qualitative interviews, cohort analyses, systematic reviews, and case studies conducted between 2016 and 2024.

Table 1. Characteristics of Included Studies on Ransomware Attacks in Healthcare Institutions (2016–2024).

| Study | Year | Study Type | Key Focus | Scope |
|---|---|---|---|---|
| **[34]** | 2023 | Qualitative interview-based study | Impacts on acute care and recovery | Experiences from emergency professionals in major hospital attacks, 2017-2022 |
| **[21]** | 2022 | Cohort study | Trends in attacks | 374 ransomware attacks on US healthcare organizations, 2016-2021 |
| **[15]** | 2023 | Review paper | Mechanics, impacts, and prevention | Global healthcare incidents, 2017-2022 |
| **[33]** | 2022 | Systematic review | Cybersecurity threats | US healthcare organizations, pharmaceutical companies, and clinics |
| **[11]** | 2022 | Theoretical proposal | Mitigation architecture | General healthcare systems |

| | | | | |
|---|---|---|---|---|
| **[28]** | 2016 | Narrative review | Federal responses | US healthcare ransomware trends up to 2016 |
| **[7]** | 2023 | Cohort study | Regional disruptions | 19,857 ED visits in two adjacent US urban EDs during a one-month attack |
| **[31]** | 2021 | Systematic survey/review | Risks, solutions | Worldwide healthcare systems up to 2021 |
| **[8]** | 2017 | Review and case analysis | Vulnerabilities, responses | 14 US hospital incidents, spring 2016 |
| **[19]** | 2023 | Retrospective comparative analysis | Hospital characteristics | US short-term acute care hospitals, 2016-2021 |
| **[23]** | 2020 | Review article | Trends, implications | International data, emphasis on US/EU |
| **[4]** | 2024 | Narrative review | Surge and initiatives | US healthcare incidents, 2020-2024 |
| **[10]** | 2023 | Case study | Obstetric division challenges | Single hospital obstetric incident |
| **[5]** | 2024 | Perspective article | Contingency planning | General US healthcare facilities |
| **[3]** | 2016 | Opinion article | Ethical hacking | Healthcare software security |
| **[27]** | 2017 | Review article | Infections, mitigation | US healthcare facilities, mid-2010s |
| **[12]** | 2017 | Review paper | Threats, prevention | US medical practices |
| **[13]** | 2017 | Blog post analysis | WannaCry lessons | UK NHS incident, 2017 |
| **[6]** | 2017 | News article/commentary | Global spread | WannaCry impact on the UK NHS and worldwide |
| **[20]** | 2017 | Case study | Guidelines, WannaCry | UK NHS incident, 2017 |

The provided studies are dated 2016-2024 and concern primarily the context of US and UK healthcare, including some review articles, cohort and case studies, as well as theoretical proposals. Real-world examples, e.g., the 2017 WannaCry attack and numerous disruptions of some US hospitals, are used to provide empirical data, which prioritizes vulnerabilities and operational effects over quantitative modeling.

### 3.2 Thematic Findings

3.2.1 Key Vulnerabilities in Healthcare Ransomware Attacks

The healthcare facilities are always vulnerable to human, technical, and structural vulnerabilities that facilitate the ransomware infiltration. Phishing and social engineering tricks use the lack of staff training, which results in initial access due to the misleading email or attachment, which is observed in various studies of attack vectors [15, 31, 34]. Outdated infrastructure, which did not implement modern security measures, allowing encryptions to pass without detection, especially in networked medical equipment and electronic health records, and the use of legacy and untested software, only increases the risks [13, 20, 28]. A weak network segmentation enables lateral movements of attackers, and a weak integration of ICT and clinical teams slows the detection process; both problems are worsened in a resource-heavy environment such as a rural hospital [19, 33]. Exposure in digital expansions, including the use of commercial vendor systems with little in-house expertise, is also increased by structural dependencies [11, 27].

#### 3.2.2 Operational and Patient Care Impacts

Ransomware attacks have a massive impact on healthcare delivery, requiring the use of manual processes and delays in vital care provision. The patient census in the neighboring emergency departments during a one-month attack period increased to 7039 and 6114 during attack and recovery respectively, with an increase in ambulance arrivals, a longer waiting room time, patients leaving the emergency department without care increased, the total patient length of stay raised, and county-wide EMS diversion increased, accompanied by worse acute stroke statistics of 6704 patient visits in the postattack period [7]. Acute care is characterized by the locked EHRs, which cause ambulance diversion, delays in treatments, and endanger vulnerable groups, and this is demonstrated by obstetric units, in which system crashes disrupted real-time monitoring in the delivery [10, 34]. Institutionally, they pay ransom demands (e.g., 40 Bitcoins worth 17,000 in one instance), recovery fees, lost revenue because of downtime, and regulatory fines, exposures incurred by institutions impacting almost 42 million patients between 2016 and 2021 [8, 21]. Regional spillover strains facilities that were not affected, and psychological stress on workers and reputational losses are reducing the resilience in the long-run [4, 23]. Confidence: Strong (consistent results with reasonable quality of design).

#### 3.2.3 Financial and Data Security Consequences

Attacks cause high economic costs and lead to the destruction of data integrity, with the dynamics of increased frequency of attacks in the period 2016-2021 and greater breaches in multi-facility organizations [21]. Net operating losses are caused by ransom payments in Bitcoin, remediation and backlog costs, especially in profitable trauma and obstetric centers [15, 19]. Information security breaches endanger valuable patient data, which is likely to result in the loss of privacy and trust, since encrypted data cannot be accessed to view health history and financial records [11, 27]. The impact on smaller, rural non-profits is increased because recovery resources are scarce, unlike with larger ones, which have more absolute losses [23]. Confidence: Moderate (usually consistent but restricted situations).

#### 3.2.4 Prevention and Mitigation Strategies

The findings are united around multi-layered defenses that focus on human and technical protection. Extensive training to identify phishing lowers entry points, which is accompanied by periodic patching of old systems and segmenting the network to limit the spread [4, 28, 34]. Offline, immutable backups can facilitate recovery without cost, whereas incident response plans can facilitate coordination of ICT and clinical activities and endpoint detection tools to isolate at an early stage [5, 20, 31]. Risk transference architectures transfer sensitive data to secure stores, and proactive vulnerabilities are identified through ethical hacking; policy interventions are focused on under-resourced hospitals with an upgrade [3, 11, 19].

In critical disease settings, such as obstetrics, continuity will be guaranteed thanks to manual protocols and simulations [10]. Credibility: Moderate (usually consistent but very little empirical testing).

### 3.2.5 Trends and High-Profile Case Examples

Attacks have become more sophisticated as 374 attacks in 2016-2021 have increased twice a year and against bigger systems [21]. In 2017, a WannaCry attack disrupted over 60 UK NHS trusts, canceling thousands of appointments, redirecting ambulances through unpatched Windows exploits (where 200,000 systems in 150 countries, including a hospital in Canada, were compromised) [6, 13, 20]. In the US alone, 14 hospitals in 2016 paid ransom to gain access to records, and the 2020 Ryuk campaign on Universal Health Services (and resulting outages), and 2023 Midwestern attacks (when surgeries were halted) [4, 8, 15]. These demonstrate the trends around the world in the state of chaos in operations and the necessity of a joint reaction. Confidence: Strong (mainly consistent results with adequate quality of design) (**Table 3**).

### 3.3 Summary of Evidence

**Table 2** shows a summary of the major vulnerabilities, operational implications, financial outcomes, mitigation measures, and high-profile incidents of ransomware attacks in healthcare facilities through the evidence-based recent cohort studies, reviews, and case studies.

Table 2. Summary of Evidence on Ransomware Attacks in Healthcare Institutions, including Vulnerabilities, Impacts, Consequences, Mitigation Strategies, and Trends.

| Theme | Key Finding | Population Applicability | Effect Direction | Confidence Level | Supporting Studies |
|---|---|---|---|---|---|
| **Key Vulnerabilities** | Phishing as primary entry; legacy systems enable encryption (e.g., unpatched Windows in WannaCry) | US/UK hospitals and clinics (matches the question population of healthcare institutions) | Negative (increased risk) | Strong | [15, 31, 34] |
| **Operational and Patient Care Impacts** | Patient census increased from 6114 preattack to 7039 during attack/recovery; delays in stroke care | Urban US emergency departments adjacent to attacked systems (matches the question population) | Negative (disruptions) | Strong | [7, 10, 34] |
| **Financial and Data Security Consequences** | Exposure of 42 million patients' data; $17,000 Bitcoin ransom in one case | Large US multi-facility organizations (matches question population) | Negative (losses, breaches) | Moderate | [8, 21, 23] |
| **Prevention and Mitigation Strategies** | Offline backups and training reduce downtime; | General healthcare facilities, | Positive (mitigation) | Moderate | [11, 19, 28] |

| | | | | | |
|---|---|---|---|---|---|
| | network segmentation limits the spread | emphasis on rural/non-profits (matches question population) | | | |
| **Trends and High-Profile Cases** | Attacks doubled from 2016 to 2021; WannaCry affected 60+ NHS trusts, canceling thousands of appointments | Global healthcare focused on the UK/US (matches the question population) | Negative (escalation) | Strong | [6, 13, 20] |

## 4. Discussion

### 4.1 Principal Findings and Their Interpretation

The synthesis has shown that ransomware has become a widespread menace to healthcare, where phishing vulnerabilities and legacy systems not only facilitate primary breaches but additionally spread in networks, which also accounts for the disruptions reported in the region (the 6114 to 7039 patient census overflows in non-affected emergency departments) [7]. This trend arises since the single points of failure in the healthcare sector, as the result of an always-on digital ecosystem that is aimed at facilitating uninterrupted access to data, gives way to unpatched software, such as WannaCry abusing Windows vulnerabilities, resulting in fast encryption that propagates further than the initial target and imposes a significant strain on other facilities because of ambulance diversion and delayed stroke care provision [13]. Mechanically, the attacks rely on social engineering around circumventing technical barriers, with the human factor (e.g., clicks on phishing links) being triggered off by malware encrypting files within seconds to minutes to block electronic health records needed to make a real-time decision [27]. No articles address more biologically or physiologically, including the effect of delays on patient outcome through interrupted observation, which is one of the gaps in the association of cyber disruptions with clinical outcomes, e.g., mortality rates. Vulnerability and impact trends are expected to be very likely because of overlaps between cohort study and case analyses in matched populations (US/UK hospitals), but probable in prevention efficacy, since intervention approaches such as offline backups have rational potential but are not assessed randomly. All these findings contribute to the state of knowledge by revealing the effects of the institutional size of impacts, where larger systems experience increased data exposure (42 million patients), whereas smaller rural systems experience existential resource pressures, which are not seen in isolated research [19, 21].

### 4.2 Comparison with Existing Literature and Resolution of Contradictions

Results are consistent with the existing literature on cyber threats, including Ponemon Institute data used in the reviews that indicate that 89% of healthcare organizations faced breaches, supporting the presence of ransomware to leverage IIT adaptation following the incentives of Meaningful Use without parallel security increase [27]. This regularity highlights the mechanistic strength: the popularity of phishing (observed in 85% of attacks through unpatched vulnerabilities) is consistent with the results of previous research, which suggests that human-technical interaction is a force behind the attack regardless of industry [28]. Hospital risk profiles are also prone to contradictions; a larger, more profitable hospital is more targeted as it has more high-value data, whereas a smaller rural non-profit is more vulnerable because of the lack of resources, which could also be attributed to the selection bias in attack reporting; those in urban areas may under-report minor incidents, which makes them seem more resilient [19]. Population heterogeneity is not supported by evidence, but it is a difference in methodology: cohort studies aggregate

data about the whole national level, which implies scale [21], as compared to qualitative interviews about grassroots strains in under-resourced environments [34]. Publication bias exposes high-profile cases to amplification by the media (unlike null cases in prepared institutions), such as the case of WannaCry (causing impact on 60+ NHS trusts) [6]. Recent research (2023-2024) based on real-time ED indicators goes beyond the news analysis of 2016-2017, and it presents more evidence of the continued impact and confirms the previous trends with more detailed data [4].

### 4.3 Practical Implications

The patching and segmentation federal funding justification would prevent the 6114-to-7039 census spikes previously experienced in the urban spillovers, and focus on these safety-net providers under conditions of resource inequity [7, 19]. Cyber-attacks in high-stakes units such as obstetrics or emergency departments should inform patients about possible delays through cyber-attacks, and manual-based protocols implemented through simulation training to facilitate constant monitoring should be implemented, particularly when dealing with at-risk groups such as pregnant individuals who are prone to real-time disruptions [10]. Leadership in the field of public health should be the subject of population-level intervention, such as the mandatory training on HIPAA alignment to overcome the human component of phishing, which can be applied to all facilities in the USA and the UK, but is necessary in multi-site organizations with access to 42 million patient records [21]. Regulatory considerations question the status quo, because no-risk risks, presented by the global WannaCry spreading to 150 countries, suggest that not all institutions suffice to provide offline backups and perform ethical hacking; rather, coordinated frameworks require it [3, 6]. There are caveats: the implications are based on the US/UK context, and more evidence should have been found on low-resource global contexts to enable assured extrapolation to other matched populations.

### 4.4 Strengths and Limitations

The strengths of this review are that the search encompassed the use of numerous databases with different types of studies, such as cohorts and cases, which have allowed the development of a solid thematic synthesis of the vulnerabilities and impacts in healthcare-specific settings. Emphasis on extracted data focuses on structured knowledge, such that it can be compared more easily. Included study limitations include the US/UK focus, as it may not capture the global differences and use of self-reported or aggregate data, without using standard measures of recovery times. A lot of them are reviews or stories, restraining causal inferences. Limitations of the review include abstract-based screening that can be insensitive to the nuances, and no formal risk-of-bias assessment, but thematic consistency helps lessen this aspect. Extraction completeness presupposes the accuracy of the abstracts, and pre-2016 data exclusion limits the historical trends.

## 5. Gaps and Future Directions

The synthesis reveals mechanistic lapses among the interference of ransomware and clinical outcomes, including how encrypted data increases mortality during an emergency, which has not been addressed due to the operational emphasis [34]. The longitudinal studies that monitor the postattack measures of patient safety, such as stroke delay that still occurs after 6704 postattack visits, are lacking, so the full impact cannot be assessed [7]. The populations that are underrepresented are those who use non-US/UK institutions, and global rural clinics do not have data, despite suggesting vulnerability [19]. The problem of contradictions in the risk profile between small and large hospitals is still not resolved because of reporting bias [21]. Prospective cohort studies in varied settings should be conducted in future studies using standardized exposure (e.g., attack simulation metrics) and outcome (e.g., harmonized downtime measures) to directly assess prevention in precise question sets. A possible technological solution to sparse empirical testing of strategies would be methodological advances such as AI-based threat modeling [31].

## 6. Conclusion

Ransomware attacks have had devastating effects on healthcare institutions due to vulnerable opportunities such as phishing and unpatched legacy systems that have resulted in high rates of 42 million patient data exposure and operational spikes of 6114-7039 emergency visits per disruption. These impacts are propagated on a regional level, slowing acute care among similar groups of US and UK hospitals and clinics, and prevention, through offline backups and training, is resiliently mitigative without stimulating additional extortion. Cohort and case evidence have high confidence in these trends, though limited to urban and vastly Western situations, which is somewhat representative of the overall population of questions in the rest of the world, and which should be avoided except in generalization to less urbanized or non-Western environments. The uncertainty that is of the utmost concern is to measure long-term patient harm, i.e., deteriorations in stroke metrics in terms of mortality, which mechanistic studies in the future ought to address. Finally, this synthesis shows the fundamental importance of cybersecurity in the protection of lives, and the need to change the policy and practice towards preventative investment should help to improve the resilience against existential threats in an ever-digitized healthcare environment and vulnerable care delivery.

## Statements and Declarations

### Funding Statement

There was no outside financing for this work.

### Conflict of Interest

The authors do not state any conflict of interest.

### Author Contributions

The study was created by the author, who conducted the literature search and wrote the manuscript. The final version was revised and accepted by the author.

### Data Availability Statement

The data analysis cannot be done in this article because no new data were developed or studied. This research is a narrative review.

## Author Biography

*Kranthi Kumar Asike Parameshwar* is currently a doctoral student at Indiana Wesleyan University, DeVoe School of Business, specializing in Technology and Leadership. He began his doctoral studies in August 2023. He previously earned a Master of Business Administration in Enterprise Resource Planning (ERP) from Lamar University, Beaumont, Texas, in 2016. His academic interests lie in the intersection of business, technology, and leadership, with a focus on advancing organizational systems through innovative technological solutions.

## REFERENCES:

1. Adil M., Khan M.K., Kumar N., Attique M., Farouk A., Guizani M.Jin Z.J.I.I.o.T.J., "Healthcare Internet of Things: Security threats, challenges, and future research directions", 2024. 11,(11): p. 19046-19069.
2. Aldosari B.J.C., "Cybersecurity in healthcare: New threat to patient safety", 2025. 17,(5),
3. AvignoneIn R., "Ethical hacking a vital necessity to fight against healthcare randsomware", Medical Economics, 2016.https://www.medicaleconomics.com/view/ethical-hacking-vital-necessity-fight-against-healthcare-randsomware
4. Bock A., *As Ransomware Attacks on Health Care Surge, Here's What Clinicians and Health Systems Can Do*. 2024.
5. Butcher L.J.P.L.J., "Ransomware Attacks Will Keep Coming—What Physician Leaders Should Do", 2024. 11,(4),
6. Collier R., *NHS ransomware attack spreads worldwide*. 2017, CMAJ.

7. Dameff C., Tully J., Chan T.C., Castillo E.M., Savage S., Maysent P., Hemmen T.M., Clay B.J.Longhurst C.A.J.J.n.o., "Ransomware attack associated with disruptions at adjacent emergency departments in the US", 2023. 6,(5): p. e2312270.
8. Farringer D.R.J.S.U.R., "Send us the bitcoin or patients will die: Addressing the risks of ransomware attacks on hospitals", 2016. 40: p. 937.
9. Force R.T.J.I.S.G., "Combating ransomware", 2021,
10. Gabbay-Benziv R., Ben-Natan M., Roguin A., Abbou B., Ofir A., Klein A., Dahan-Shriki D., Hallak M., Kessel B., Dudkiewicz M.J.I.J.o.G.Obstetrics, "When the lights go down in the delivery room: Lessons from a ransomware attack", 2023. 162,(2): p. 562-568.
11. Gopinath S.Olmsted A.J.a.p.a., "Mitigating the effects of ransomware attacks on healthcare systems", 2022,
12. Gupta G.Tripathi K.J.I.E.R.J., "Study on ransomware attack and its prevention", 2017. 3,(5): p. 260-262.
13. Hills M., "Lessons from the NHS ransomware calamity", 2017,
14. Jeelan P.M., Saini R., Parida S., Minhas D., ManashreeAgarwal A. *The Threat Landscape of Ransomware in Critical Infrastructure: An Optimization Perspective*. in *2025 International Conference on Automation and Computation (AUTOCOM)*. 2025.
15. Kesarwani A.Gochhayat S.J.J.o.S.R., "Ransomware attacks in the healthcare industry", 2023. 12,(4),
16. Kruse C.S., Frederick B., Jacobson T., Monticone D.K.J.T.Care H., "Cybersecurity in healthcare: A systematic review of modern threats and trends", 2017. 25,(1): p. 1-10.
17. Malenfant T., *Impact of ransomware attacks on healthcare*. 2021: Utica College.
18. Malik V., Khanna A., Sharma N.J.I.J.o.G.I.Solutions, "Trends in ransomware attacks: analysis and future predictions", 2024,
19. McGlave C.C., Nikpay S.S., Henning-Smith C., Rydberg K.Neprash H.T.J.H.A.S., "Characteristics of short-term acute care hospitals that experienced a ransomware attack from 2016 to 2021", 2023. 1,(3): p. qxad037.
20. Mishra D.J.I.J.o.E.R.Technology, "Cyber Security Guidelines for Healthcare Providers Threats and Defense from Ransomware", 2017. 6,(12),
21. Neprash H.T., McGlave C.C., Cross D.A., Virnig B.A., Puskarich M.A., Huling J.D., Rozenshtein A.Z.Nikpay S.S. *Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021*. in *JAMA Health Forum*. 2022.
22. Organization W.H., *Cybersecurity and privacy maturity assessment and strengthening for digital health information systems*. 2025, World Health Organization. Regional Office for Europe.
23. Palicz T., Sas T., Tisóczki J., Bencsik B.Joó T.J.O.H., "“Your money or your life!”–Ransomwares in healthcare information systems", 2020. 161,(36): p. 1498-1505.
24. Parmar M.Miles A. *Cyber security frameworks (CSFs): An assessment between the NIST CSF v2. 0 and EU standards*. in *2024 Security for Space Systems (3S)*. 2024. IEEE.
25. Secur I.J.A.J., "Cost of a Data Breach Report 2024", 2024. 27: p. 2025.
26. Shahzadi A., Ishaq K., Dogar A.B., Khan J.A., Mylonas A., Nawaz N.A., Yasin A.Khan F.A.J.P.C.S., "Safeguarding the healthcare sector from ransomware attacks: insights from a literature review", 2025. 11: p. e3073.
27. Spence N., Paul III D.P.Coustasse A., "Ransomware in healthcare facilities: the future is now", 2017,
28. Stewart, "Feds focus on healthcare ransomware attacks", Medical Economics, 2016.https://www.medicaleconomics.com/view/feds-focus-healthcare-ransomware-attacks
29. Sushma K., Viji C., Rajkumar N., Ravi J., Stalin M.Najmusher H.J.P.C.S., "Healthcare 4.0: A review of phishing attacks in cyber security", 2023. 230: p. 874-878.

30. Tellez Salinas C., "Ransomware in the EU: Assessment of the Threat Landscape and Cybersecurity Governance", 2024,
31. Thamer N.Alubady R. *A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research*. in *2021 1st Babylon international conference on information technology and science (BICITS)*. 2021. IEEE.
32. Triplett W.J.J.C.Journal I.T., "Cybersecurity vulnerabilities in healthcare: a threat to patient security", 2024. 2,(1): p. 15-25.
33. Triplett W.J.J.o.B., TechnologyLeadership, "Ransomware attacks on the healthcare industry", 2022. 4,(1): p. 1-13.
34. van Boven L.S., Kusters R.W.J., Tin D., van Osch F.H.M., De Cauwer H., Ketelings L., Rao M., Dameff C.Barten D.G., "Hacking Acute Care: A Qualitative Study on the Health Care Impacts of Ransomware Attacks Against Hospitals", Ann Emerg Med, 2024. 83,(1): p. 46-56.