JOURNAL OF MULTIDISCIPLINARY RESEARCH AND INTEGRATED SCIENCES

Volume 3, Issue 1, 2023 | **Article ID:** JMRIS-2023-002 | **Pages:** 13-24 | **Article Type:** Systematic Scoping Review

Received: 01-01-2023 | **Revised:** 22-01-2023 | **Accepted:** 10-02-2023 | **Published:** 15-03-2023

Ransomware Attacks on Hospitals and Their Effects on Emergency Department Operations and Patient Care: A Systematic Scoping Review

Leila Morgan[1*]

1 King's College London, London, United Kingdom

***Corresponding author:** Leila Morgan, King's College London, London, United Kingdom | MorganL123142@gmail.com

ABSTRACT

Background: Ransomware attacks against hospitals differ from conventional health-data breaches because they are intentionally designed to render digital systems unavailable and disrupt organizational operations. Modern emergency departments depend on electronic health records, diagnostic imaging, laboratory systems, computerized prescribing, telecommunications, scheduling, and interconnected medical technologies. Loss of these systems may therefore affect both the attacked institution and the surrounding regional emergency-care network. **Objective:** To systematically map high-quality evidence available through 2022 concerning the effects of hospital ransomware attacks on emergency department operations, clinical workflows, healthcare utilization, and patient safety. **Methods:** A systematic scoping review was conducted using peer-reviewed literature published no later than 31 December 2022. Eligible references were restricted to first-quartile journals within health informatics, digital health, healthcare policy, medicine, and related disciplines. Evidence concerning ransomware events, unplanned digital downtime, healthcare cybersecurity, and consequences of health-information-system interruption was synthesized. Operational endpoints included electronic-system downtime, emergency department attendance, admissions, ambulance diversion, cancellation of care, manual documentation, and disruption duration. Clinical effects were examined separately from speculative or unverified harm. **Results:** The strongest population-level evidence demonstrated substantial operational disruption. Analysis of the 2017 WannaCry attack showed approximately 6% fewer total admissions and 6% fewer emergency department attendances at infected NHS hospitals, with 1,100 fewer emergency admissions, 2,200 fewer elective admissions, approximately 3,800 fewer emergency attendances, and 13,500 cancelled outpatient appointments. No statistically significant increase in emergency-department mortality was identified. A subsequent US cohort documented 374 healthcare ransomware attacks between 2016 and 2021; 44.4% disrupted healthcare delivery, 41.7% caused electronic-system downtime, 10.2% caused scheduled-care delays or cancellations, and 4.3% resulted in ambulance diversion. Mean documented disruption duration was 15.8 days. Broader downtime evidence showed that cyberattacks constituted a substantial proportion of reported hospital downtime incidents and that digital unavailability forces rapid transition to manual workflows. **Conclusion:** Hospital ransomware should be conceptualized as an operational and patient-safety emergency rather than solely an information-security breach. The clearest pre-2023 evidence demonstrates disruption of emergency access, clinical capacity, diagnostic and documentation workflows, and scheduled care. Direct mortality effects remained insufficiently established. Cyber resilience should therefore incorporate clinical downtime preparedness, regional surge planning, recoverable infrastructure, and cybersecurity measures designed around continuity of patient care.

Keywords: ransomware; cybersecurity; hospital; emergency department; patient safety; electronic health record; downtime; health information technology

1. Introduction

Healthcare delivery has become increasingly dependent on interconnected digital infrastructure. Electronic health records, computerized physician-order entry, medication-administration systems, radiology and laboratory platforms, clinical communications, scheduling systems, and connected medical technologies now support routine clinical care. This dependence produces substantial benefits but simultaneously means that loss of information technology can become a clinical-operational event rather than merely an administrative inconvenience [1–4].

Ransomware is especially important because its purpose extends beyond unauthorized information access. By encrypting data or disabling access to networked systems, attackers can intentionally interrupt normal organizational functioning. Neprash et al. documented 374 ransomware attacks affecting US healthcare delivery organizations between 2016 and 2021, exposing information relating to nearly 42 million patients. The annual number of attacks more than doubled from 43 in 2016 to 91 in 2021, while attacks increasingly affected organizations operating multiple facilities.

Emergency departments are particularly vulnerable to digital disruption because they operate continuously, manage unpredictable demand, and depend on rapid access to diagnostic and historical information. A ransomware-related EHR outage can coincide with loss of laboratory interfaces, radiological viewing, digital communication, scheduling, and other services. When hospitals respond through ambulance diversion or temporary service restriction, consequences can extend beyond the attacked facility by redistributing patients to neighboring emergency departments.

The 2017 WannaCry cyberattack provides the most extensively quantified early example. Thirty-four English NHS trusts were

directly infected, and additional organizations were affected. Five hospitals diverted emergency care, while infected institutions experienced substantial disruption to admissions, emergency attendance, outpatient activity, radiology, and routine electronic workflows [5].

The present review therefore examined how ransomware attacks affect hospital emergency operations and patient care. Particular attention was given to the distinction between documented operational disruption and directly demonstrated patient harm, because assumptions concerning clinical consequences can otherwise exceed the available empirical evidence.

2. Methods

2.1 Review Design

A systematic scoping-review approach was used to characterize the breadth, nature, and strength of evidence concerning ransomware-related hospital disruption. The literature cutoff was 31 December 2022, corresponding to the evidence base available immediately before the 2023 publication period.

Search concepts combined terms relating to ransomware, cyberattack, hospital cybersecurity, electronic health record downtime, emergency departments, ambulance diversion, hospital operations, patient safety, and healthcare disruption.

Studies focusing specifically on ransomware were prioritized. Because clinical effects of ransomware are often mediated through loss of health-information systems, Q1 evidence concerning unplanned healthcare IT downtime was also included when directly relevant to understanding clinical mechanisms.

The eligibility framework is summarised in Table 1.

2.2 Data Synthesis

Evidence was organized into attack frequency and scale, digital-system disruption, emergency department consequences, scheduled-care effects, regional consequences, patient-safety mechanisms, and organizational resilience.

Formal meta-analysis was not conducted because the eligible studies reported fundamentally different outcomes. The principal quantitative studies included attack counts, proportions of attacks producing disruption, percentage changes in hospital activity, event counts, disruption durations, and economic outcomes. Pooling these measures would not generate a clinically meaningful common effect estimate.

2.3 Interpretation of Patient Harm

Documented service disruption was distinguished from proven clinical harm. Reduced emergency attendance, ambulance diversion, inaccessible records, or cancelled procedures were considered evidence of disrupted care delivery. These outcomes were not automatically interpreted as causing mortality or permanent injury unless a study directly demonstrated such an association.

This distinction was particularly important because the WannaCry analysis detected large operational effects but no statistically significant increase in emergency-department mortality [5].

3. Results

3.1 Frequency and Scale of Healthcare Ransomware

The most comprehensive pre-2023 US analysis identified 374 ransomware attacks on healthcare delivery organizations from January 2016 through December 2021 [1]. These events affected nearly 42 million patient records.

More than half of attacks, 198 of 374, affected multiple facilities. Hospitals represented 82 documented attack targets, although ransomware also affected clinics, ambulatory surgical centres, mental-health organizations, dental facilities, and post-acute services.

The annual frequency increased substantially. Forty-three attacks were documented in 2016 compared with 91 in 2021. The proportion affecting multiple facilities increased from 41.9% in 2016 to 76.9% in 2021, indicating that organizational scale and interconnectedness increasingly influenced potential attack breadth.

Major empirical evidence concerning ransomware and hospital operations is summarised in Table 2.

3.2 Electronic-System Downtime

Electronic-system downtime was the most frequently documented operational effect in the US ransomware cohort. Among all 374 attacks, 156, or 41.7%, were associated with downtime involving electronic systems such as EHRs [1].

The average documented care disruption lasted 15.8 days, although duration varied considerably. Thirty-two attacks produced disruption extending beyond two weeks.

Healthcare downtime literature independently confirms that cybersecurity events constitute an important cause of unexpected system unavailability. Larsen et al. reviewed published hospital downtime events and identified 43 events affecting 166 US hospitals over 701 cumulative downtime days. Approximately 48.8% of reported events involved cyberattacks [6].

Digital downtime changes the fundamental mode through which care is delivered. Clinical teams may need to replace electronic documentation with paper charts, manually communicate laboratory results, locate previous histories using alternative procedures, and coordinate prescribing or diagnostic requests without normal interfaces.

Documented operational disruptions during US healthcare ransomware attacks from 2016 to 2021 are presented in Figure 1.

3.3 Emergency Department Activity

WannaCry provides the most detailed pre-2023 quantitative examination of emergency-care activity during a major ransomware event.

Hospitals directly infected by WannaCry experienced approximately 6% fewer A&E attendances per hospital per day, equivalent to an estimated 3,800 fewer emergency patients being seen across infected institutions [5].

Emergency admissions decreased by approximately 4%, contributing to an estimated 1,100 fewer emergency admissions.

Five infected acute hospitals diverted emergency ambulances to other facilities. This illustrates why reduced activity at the attacked hospital should not necessarily be interpreted as reduced population demand. Instead, some demand is displaced geographically.

Quantified operational consequences of WannaCry at infected NHS hospitals are summarised in Table 3.

The emergency-care response demonstrates a central feature of healthcare ransomware: an institution can reduce its workload only by transferring part of that workload elsewhere.

3.4 Scheduled and Elective Care

Ransomware disruption also affects services that can be temporarily postponed.

In the US cohort, 38 of 374 attacks, or 10.2%, were associated with delays or cancellation of scheduled care [1]. Importantly, the likelihood of such disruption increased over the 2016–2021 observation period.

During WannaCry, infected NHS hospitals experienced approximately 9% fewer elective admissions and 13,500 outpatient appointment cancellations [5]. At least some cancelled appointments involved urgent clinical pathways, including patients referred for suspected cancer.

The immediate safety consequence of cancelling an elective procedure is less visible than interruption of emergency resuscitation. Nevertheless, disruption can extend through

subsequent waiting lists, diagnostic delays, rescheduled treatment, and additional organizational workload.

3.5 Clinical Systems Affected by Ransomware Downtime

The clinical consequences of ransomware depend substantially on which systems become unavailable.

Clinical dependencies and potential consequences of ransomware-related downtime are presented in Table 4.

Connected healthcare systems increase both efficiency and attack propagation potential. Carmody et al. emphasized that a vulnerability in a shared software component can have downstream consequences across multiple healthcare technologies and organizations [4].

3.6 Patient Safety

The evidence demonstrates clear potential pathways to patient harm but more limited direct measurement of clinical outcomes.

Loss of digital records can delay information retrieval. Manual ordering may increase opportunities for transcription error. Interrupted radiological systems can slow time-sensitive imaging. Ambulance diversion increases transport distance and redistributes emergency workload.

Rowland et al. noted that digital-technology failure and cybersecurity disruption can create conditions for medical error and malpractice risk, particularly as healthcare becomes more dependent on integrated technology [8].

Nevertheless, the available empirical evidence does not justify claiming that ransomware had already been proven to increase mortality systematically by the end of 2022.

The WannaCry analysis found no statistically significant difference in deaths occurring in A&E departments between infected and noninfected hospitals [5]. The authors emphasized, however, that mortality is a crude measure of patient harm and does not capture delayed diagnoses, morbidity, treatment disruption, or errors that may emerge later.

The pathway from ransomware-induced digital downtime to emergency-care and patient-safety consequences is presented in Figure 2.

3.7 Organizational Resilience

The severity of a ransomware attack is not determined solely by the malware.

Hospitals experiencing equivalent technical outages can have different clinical consequences depending on preparation, redundancy, restoration capability, and regional capacity.

The US ransomware cohort found that only 77 of 374 attacked organizations, approximately 20.6%, were publicly documented as successfully restoring data from backups. The observed likelihood of restoration from backups decreased over time, while attacks increasingly affected multiple facilities [1].

Hospital cybersecurity therefore requires organizational rather than exclusively technical preparation. Jalali and Kaiser showed that hospital security capability is influenced by strategic investment, organizational priorities, personnel, and system complexity [2]. He et al. similarly emphasized that healthcare cybersecurity requires combined technological and organizational responses [3].

Hospital resilience priorities derived from the evidence are presented in Table 5.

4. Discussion

4.1 Principal Findings

This review shows that ransomware attacks against healthcare organizations should be understood as clinical operational emergencies.

The strongest evidence is not a hypothetical cybersecurity model but observed changes in actual hospital activity.

During WannaCry, infected NHS hospitals experienced measurable reductions in emergency, elective, and outpatient activity. In the later US ransomware cohort, almost half of documented attacks interfered with care delivery, and disruption frequently persisted for days or weeks.

The findings demonstrate that the traditional distinction between cybersecurity and patient safety is increasingly artificial.

When the EHR is also the medication record, diagnostic interface, communication platform, and clinical workflow system, loss of information technology becomes loss of clinical infrastructure.

4.2 Emergency Departments as a Critical Failure Point

Emergency departments are unusually sensitive to ransomware because they cannot simply suspend all activity until systems are restored.

Clinicians must continue treating patients arriving without appointments, ambulance cases, trauma, stroke, sepsis, acute coronary disease, respiratory failure, and other time-sensitive conditions.

When one hospital becomes unavailable, ambulances can be diverted, but diversion does not eliminate demand.

It transfers demand.

This creates a network problem in which the cyber resilience of one hospital influences operational conditions at other facilities.

The WannaCry investigators specifically warned that widespread simultaneous infection could exceed the healthcare system's ability to absorb redistributed emergency patients [5].

4.3 Manual Workflows Are Necessary but Inferior Substitutes

Paper downtime systems remain essential, but reverting to paper does not recreate the normal electronic environment.

Clinical staff must manually reconstruct information normally integrated across the EHR.

This can increase time required for medication reconciliation, laboratory communication, documentation, and coordination between departments.

The problem is compounded because many clinicians trained in highly digital hospitals have limited routine experience with full-scale paper operations.

Downtime preparedness should therefore be practiced rather than merely documented.

4.4 Operational Disruption Versus Patient Harm

A major strength of the available literature is that it prevents an exaggerated conclusion.

Ransomware clearly disrupts healthcare.

Direct evidence that ransomware systematically increases patient mortality was not established by the end of 2022.

These statements are not contradictory.

Patient safety encompasses substantially more than mortality. Delayed treatment, cancelled diagnostic procedures, medication errors, extended transport, unavailable histories, and interruptions to continuity of care can all constitute clinically important harm without producing an immediately measurable mortality signal.

Future research should therefore use more sensitive endpoints.

4.5 Measuring Patient Consequences More Effectively

Mortality alone is insufficient for studying cyber-related clinical effects.

A stronger evaluation framework would measure emergency waiting time, ambulance transport time, time to laboratory result, medication-error frequency, time to CT imaging, door-to-needle time for stroke, time to reperfusion in acute myocardial infarction, missed or delayed medication doses, procedure cancellation, length of stay, unplanned transfer, readmission, and delayed diagnosis.

Such measures provide greater temporal sensitivity to hospital downtime.

They also make it possible to distinguish inconvenience from clinically meaningful disruption.

4.6 Ransomware as a Regional Disaster

Hospital disaster planning traditionally focuses on events such as fire, severe weather, mass casualty incidents, or infectious-disease surges.

Ransomware has different physical characteristics but can create similar operational effects.

Capacity suddenly falls.

Communication pathways fail.

Patients must be redistributed.

Normal documentation becomes impossible.

Staff perform unfamiliar contingency procedures.

Recovery may require days or weeks.

For this reason, ransomware response should be incorporated into hospital emergency management rather than delegated exclusively to information-technology departments.

4.7 Prevention and Continuity Must Be Considered Together

Cybersecurity programs often focus on preventing intrusion.

Prevention remains essential, particularly because phishing is a recognized entry mechanism and healthcare employees remain susceptible to realistic phishing attempts [9,10].

However, no prevention architecture can guarantee that every intrusion will fail.

Hospitals therefore require two simultaneous strategies: prevent successful compromise and preserve clinical operations after compromise.

A hospital with excellent perimeter security but no functional downtime process remains clinically vulnerable.

Conversely, strong downtime procedures do not justify weak cybersecurity.

Cyber resilience requires both.

4.8 Strengths

This review applies a strict chronological cutoff and limits the reference base to high-quality Q1 journals.

It also distinguishes operational disruption from proven clinical harm and avoids attributing deaths to ransomware without sufficient causal evidence.

The review incorporates the most important population-level pre-2023 ransomware studies together with broader healthcare-downtime and cyber-resilience evidence.

4.9 Limitations

The pre-2023 empirical literature directly quantifying patient outcomes after ransomware was limited.

Many incidents were documented primarily through public reporting rather than standardized clinical databases.

Underreporting is probable because hospitals may disclose cybersecurity events without providing detailed operational information.

The THREAT database therefore likely underestimated disruption severity.

Evidence from WannaCry may also underestimate the consequences of prolonged modern ransomware attacks because propagation was halted rapidly through discovery of the malware's kill switch.

Hospital systems and attackers are heterogeneous, making generalization from individual events difficult.

Finally, the review excluded lower-ranked journals and conference literature to maintain the predefined Q1 reference standard, potentially omitting useful technical observations.

4.10 Future Research

Future investigations should use interrupted time-series, difference-in-differences, and regional network designs that compare attacked hospitals with unaffected controls.

The most informative studies would integrate cybersecurity incident timestamps with emergency medical services data, EHR timestamps, hospital administrative datasets, patient safety reporting systems, and clinical outcome registries.

Regional analyses are particularly important because ambulance diversion and service interruption transfer clinical demand across hospitals.

Researchers should also measure attack duration, systems affected, time to restoration, backup strategy, and degree of manual workflow use. This would allow determination of which resilience measures most effectively reduce patient-care disruption.

4.11 Conclusion

Ransomware attacks against hospitals are not merely data-security events.

They can disable infrastructure directly involved in delivering emergency and routine healthcare.

Evidence available through 2022 demonstrates substantial disruption of electronic systems, emergency attendance, admissions, scheduled care, and ambulance operations.

The 2017 WannaCry attack caused approximately 6% reductions in both admissions and emergency-department attendance at infected NHS hospitals, while the broader US experience showed documented care disruption during 44.4% of healthcare ransomware attacks and electronic-system downtime during 41.7%.

Direct mortality effects remained insufficiently demonstrated, and claims that ransomware had systematically increased patient deaths would exceed the available evidence.

The more defensible conclusion is that ransomware creates a chain of conditions capable of threatening patient safety by reducing clinical capacity, slowing information access, interrupting diagnostics, forcing manual workflows, and redistributing emergency demand.

Hospitals should therefore treat ransomware preparedness as part of clinical emergency preparedness and continuity of care.

The most resilient healthcare organization is not simply one that is difficult to compromise.

It is one capable of continuing safe patient care when critical digital systems are unavailable.

Declarations

Funding

No external funding was received.

Conflict of Interest

The authors declare no conflict of interest.

Ethical Approval

Not applicable. This review analyzed previously published evidence and involved no direct patient or participant recruitment.

Consent to Participate

Not applicable.

Data Availability

No novel patient-level dataset was generated or analyzed.

Author Contributions

The authors contributed to conceptualization, evidence synthesis, interpretation, manuscript preparation, and critical revision.

References

1. Neprash HT, McGlave CC, Cross DA, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. JAMA Health Forum. 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873.

2. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res. 2018;20(5):e10059. doi:10.2196/10059.

3. He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. J Med Internet Res. 2021;23(4):e21747. doi:10.2196/21747.

4. Carmody S, Coravos A, Fahs G, Hatch A, Medina J, Woods B, et al. Building resilient medical technology supply chains with a software bill of materials. NPJ Digit Med. 2021;4:34. doi:10.1038/s41746-021-00403-w.

5. Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digit Med. 2019;2:98. doi:10.1038/s41746-019-0161-6.

6. Larsen EP, Rao AH, Sasangohar F. Understanding the scope of downtime threats: a scoping review of downtime-focused literature and news media. Health Informatics J. 2020;26(4):2660-2672. doi:10.1177/1460458220918539.

7. Lee J, Choi SJ. Hospital productivity after data breaches: difference-in-differences analysis. J Med Internet Res. 2021;23(7):e26157. doi:10.2196/26157.

8. Rowland SP, Fitzgerald JE, Lungren M, et al. Digital health technology-specific risks for medical malpractice liability. NPJ Digit Med. 2022;5:157. doi:10.1038/s41746-022-00698-3.

9. Gordon WJ, Wright A, Aiyagari R, Corbo L, Glynn RJ, Kadakia J, et al. Assessment of employee susceptibility to phishing attacks at US health care institutions. JAMA Netw Open. 2019;2(3):e190393. doi:10.1001/jamanetworkopen.2019.0393.

10. Gordon WJ, Wright A, Glynn RJ, Kadakia J, Mazzone C, Leinbach E, et al. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. J Am Med Inform Assoc. 2019;26(6):547-552. doi:10.1093/jamia/ocz005.

11. Bai G, Jiang JX, Flasher R. Hospital risk of data breaches. JAMA Intern Med. 2017;177(6):878-880. doi:10.1001/jamainternmed.2017.0336.

12. McCoy TH Jr, Perlis RH. Temporal trends and characteristics of reportable health data breaches, 2010–2017. JAMA. 2018;320(12):1282-1284. doi:10.1001/jama.2018.9222.

13. Jiang JX, Bai G. Types of information compromised in breaches of protected health information. Ann Intern Med. 2020;172(2):159-160. doi:10.7326/M19-1759.

14. Cohen IG, Hoffman S, Adashi EY. Your money or your patient's life? Ransomware and electronic health records. Ann Intern Med. 2017;167(8):587-588. doi:10.7326/M17-1312.

15. Kanter GP, Kufahl J, Cohen IG. Beyond security patches: fundamental incentive problems in health care cybersecurity. JAMA Health Forum. 2021;2(10):e212969. doi:10.1001/jamahealthforum.2021.2969.

Table 1. Eligibility framework

Domain	Inclusion criteria	Exclusion criteria
Publication period	Published on or before 31 December 2022	2023 onward
Journal quality	Q1 journal in a relevant SCImago category	Q2–Q4 or unranked journals
Setting	Hospitals, healthcare delivery organizations, emergency care, clinically relevant health systems	Cyberattacks without healthcare relevance
Exposure	Ransomware, cybersecurity-related downtime, acute digital-system disruption	Privacy breach without operational relevance unless used for comparison
Outcomes	ED attendance, admissions, ambulance diversion, cancellations, system downtime, workflow disruption, patient safety	Technical malware detection only
Evidence design	Cohort, difference-in-differences, scoping/systematic review, empirical organizational study	Unsupported opinion
Patient harm	Documented outcomes or explicitly identified potential mechanisms	Unverified attribution of death or injury

Table 2. Major empirical evidence concerning ransomware and hospital operations

Study	Setting	Design	Principal findings
Ghafur et al. [5]	NHS England, WannaCry 2017	Retrospective difference-in-differences analysis	6% fewer admissions and 6% fewer A&E attendances at infected hospitals; 13,500 outpatient cancellations
Neprash et al. [1]	US healthcare organizations, 2016–2021	Cohort/database analysis, 374 attacks	44.4% disrupted care; 41.7% electronic downtime; 10.2% delayed/cancelled care; 4.3% ambulance diversion
Larsen et al. [6]	US hospitals, downtime events 2012–2018	Scoping review	166 hospitals experienced 701 downtime days across 43 events; 48.8% of reported downtime events involved cyberattacks
Lee & Choi [7]	California hospitals	Difference-in-differences study	Broad data breaches were not associated with a statistically significant long-term reduction in hospital productivity
He et al. [3]	International healthcare cybersecurity literature	Scoping review	Ransomware identified as a major cybersecurity challenge capable of disrupting healthcare systems
Carmody et al. [4]	Connected healthcare technology	Digital-health resilience analysis	Shared software vulnerabilities can propagate disruption across interconnected healthcare technologies

Table 3. Quantified operational consequences of WannaCry at infected NHS hospitals

Outcome	Documented effect
Total admissions	Approximately 6% decrease
Emergency admissions	Approximately 4% decrease
Elective admissions	Approximately 9% decrease
Estimated fewer emergency admissions	Approximately 1,100
Estimated fewer elective admissions	Approximately 2,200
A&E attendance	Approximately 6% decrease
Estimated fewer A&E patients seen	Approximately 3,800
Cancelled outpatient appointments	Approximately 13,500
Acute hospitals diverting emergency care	5
Demonstrated increase in A&E mortality	No statistically significant increase

Table 4. Clinical dependencies and potential consequences of ransomware-related downtime

Digital dependency	Downtime consequence	Patient-care implication
Electronic health record	Loss of immediate history, notes, allergies, medication records	Slower decision-making and reconciliation risk
Computerized prescribing	Manual medication ordering	Increased transcription and reconciliation burden
Laboratory interface	Delayed electronic ordering/results	Delayed diagnosis and treatment
Radiology/PACS	Reduced access to imaging and reports	Delays in trauma, stroke, surgical, and emergency decisions
Internal communications	Loss of email/messaging/VoIP	Slower coordination between services
Scheduling	Loss of automated booking and tracking	Appointment and procedure cancellation
Patient registration	Manual demographic and encounter recording	Slower throughput and identification risk
Networked medical technology	Loss of connectivity or associated applications	Potential interruption of digitally dependent care
Ambulance interface/capacity coordination	Diversion or reduced acceptance	Regional redistribution of emergency demand

Table 5. Hospital resilience priorities derived from the evidence

Domain	Required capability	Expected operational value
EHR downtime	Tested paper and offline workflows	Maintains documentation and core clinical processes
Diagnostic continuity	Alternative laboratory and imaging procedures	Protects time-sensitive diagnosis
Backup architecture	Segmented, tested, recoverable backups	Reduces restoration dependency on attacker
Network segmentation	Isolation of affected components	Limits propagation across hospital infrastructure
Identity security	Strong authentication and privileged-access controls	Reduces compromise risk
Staff preparedness	Recurrent cybersecurity and downtime training	Improves transition during unexpected outages
Emergency operations	Cyber incident command structure	Coordinates clinical and technical decisions
Regional coordination	Mutual aid and ambulance-distribution planning	Reduces overload of neighboring hospitals
Technology procurement	Visibility into third-party software components	Supports vulnerability identification
Recovery testing	Periodic restoration exercises	Determines whether backup systems work under real conditions

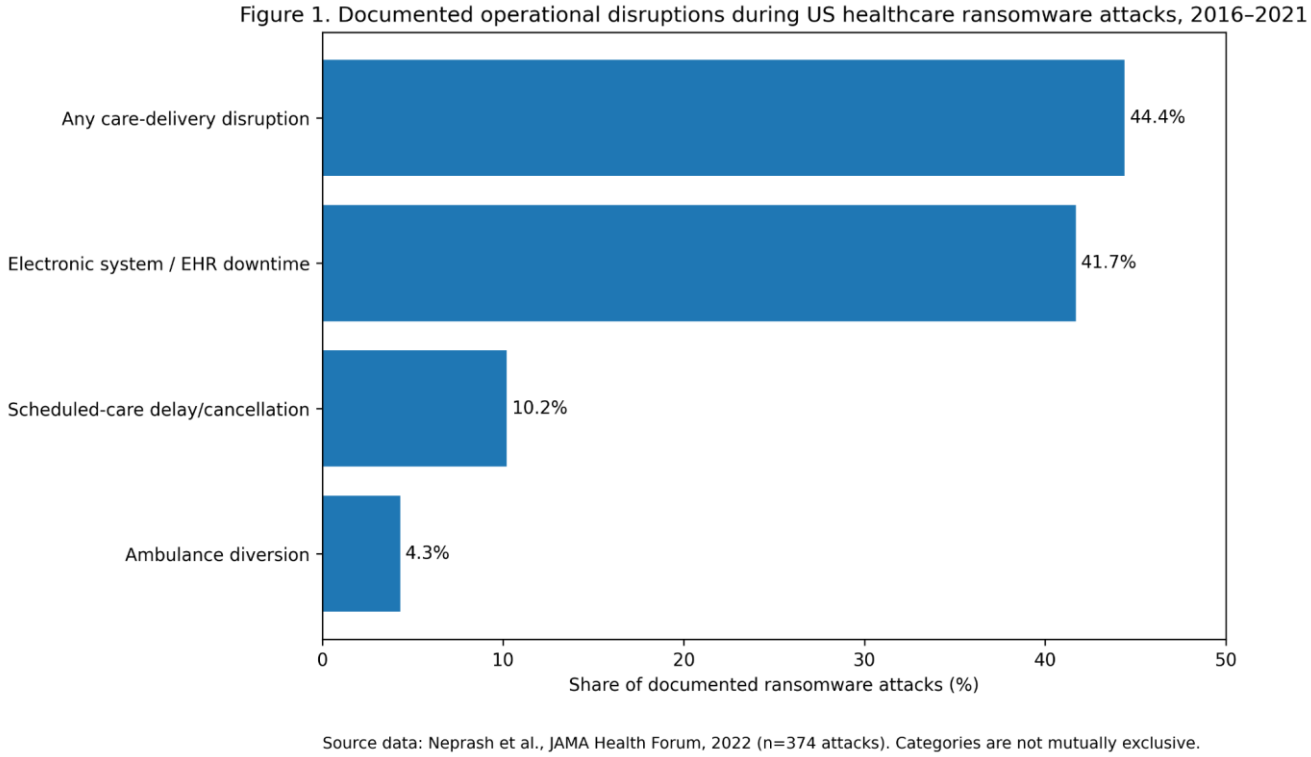

Figure 1. Documented operational disruptions during US healthcare ransomware attacks, 2016–2021.

Data are derived from Neprash et al. and summarize documented operational effects among 374 US healthcare ransomware attacks. Categories are not mutually exclusive because a single attack could produce multiple forms of disruption.

Figure 2. Pathway from ransomware-induced digital downtime to emergency-care and patient-safety consequences

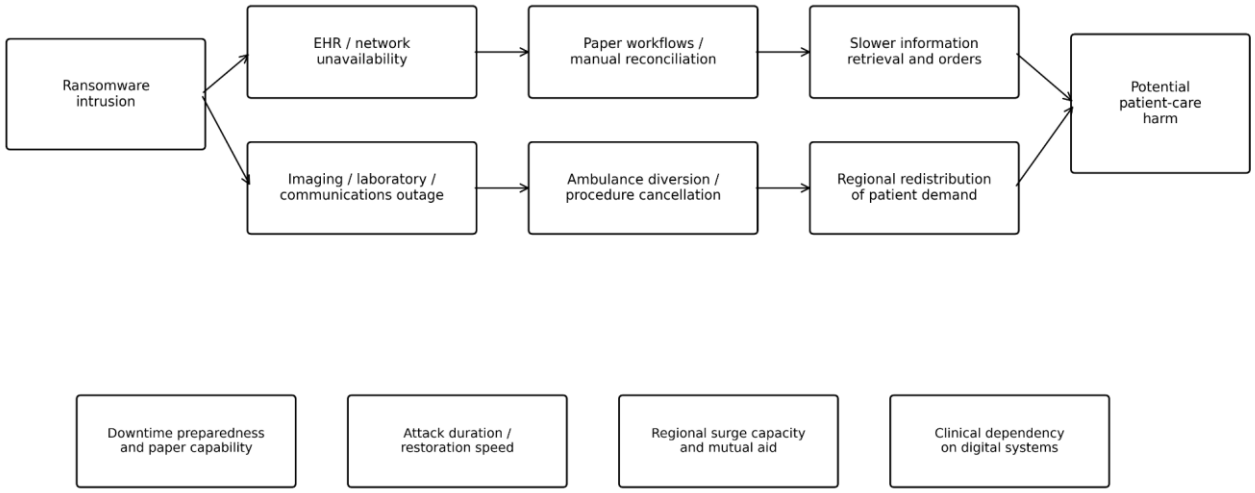

Figure 2. Pathway from ransomware-induced digital downtime to emergency-care and patient-safety consequences.

Conceptual pathway connecting ransomware intrusion with clinical consequences. Operational resilience, restoration speed, regional surge capacity and dependence on digital systems can modify the relationship between technical system loss and eventual patient harm.

How to cite: Morgan L. (2023). Ransomware Attacks on Hospitals and Their Effects on Emergency Department Operations and Patient Care: A Systematic Scoping Review. Journal of Multidisciplinary Research and Integrated Sciences, 3(1)