International Journal of Security Sciences (IJSS)
July-December-Issue, Vol. 1, No. 1 (2026) | DOI: 10.66261/nv5pz549

Article – e004

Operational Indicators of Clinical Service Disruption and Recovery Following Healthcare Ransomware Attacks: A Critical Review of Empirical Evidence

Rohit Gawde[1], Sachin Joshi[2]

[1,2] Symbiosis International (Deemed University), Pune, Maharashtra

Received: 30/08/2026 **Revision Received:** 28/09/2026 **Accepted:** 03/10/2026

ABSTRACT

Ransomware attacks against healthcare organizations can disrupt clinical services even when the immediate technical compromise is confined to information systems. Electronic health record unavailability, communication failures, diversion of emergency patients, interruption of diagnostic workflows, and dependence on manual procedures can affect service delivery both within attacked hospitals and across surrounding healthcare networks. However, the operational consequences of ransomware are not adequately represented by technical indicators such as system downtime or restoration time alone. This critical narrative review examines empirical evidence concerning healthcare ransomware incidents and identifies operational indicators that can be used to assess clinical service disruption and recovery. We draw on studies of hospital activity, emergency department spillover, emergency medical services, clinical workflows, patient outcomes, and post-incident recovery. Particular attention is given to distinguishing directly measured operational effects from broader claims that remain insufficiently supported by empirical evidence. A five-domain framework is proposed encompassing service availability, patient flow and capacity, clinical workflow continuity, patient safety and outcomes, and recovery stability. The framework separates technical restoration from operational normalization and clinical recovery. The review finds that ransomware-related disruption may extend beyond the attacked institution, that routine healthcare activity measures can reveal consequences not captured by cybersecurity reporting, and that recovery should be assessed through multiple operational indicators rather than a single restoration milestone. Further longitudinal and multicenter research is needed to establish standardized measures of healthcare service resilience following ransomware attacks.

KEYWORDS: Ransomware; healthcare cybersecurity; clinical service disruption; hospital operations; emergency departments; patient safety; cyber resilience; service recovery

1 Introduction

Healthcare organizations depend on interconnected digital systems to support clinical documentation, patient registration, diagnostic testing, medication administration, scheduling, communications, and coordination between care providers. This dependence creates substantial operational consequences when essential systems become unavailable. Ransomware attacks are particularly concerning because their effects can extend beyond the encryption of files or interruption of individual applications. Healthcare organizations may suspend elective procedures, divert emergency patients, postpone diagnostic services, and adopt manual workarounds while technical teams attempt to contain the incident and restore systems. The consequences of these disruptions cannot be understood solely through conventional cybersecurity measures.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

An organization may report that its electronic health record system has been restored, but clinical services may remain constrained by accumulated patient backlogs, incomplete records, delayed investigations, disrupted referrals, or reduced staff capacity. Conversely, a hospital may continue delivering essential services through contingency procedures despite prolonged technical unavailability. Technical system status and clinical service performance must therefore be measured separately. Ghafur et al. [1] examined the effects of the WannaCry cyberattack on National Health Service organizations in England, documenting substantial operational disruption and associated financial consequences. Subsequent research has investigated ransomware incidents across United States hospitals, including their effects on hospital operations, emergency departments, neighboring institutions, and patient outcomes [2–6].

The growing evidence base now allows a closer look at how disruption is measured and which indicators provide a useful picture of recovery. Even so, the available evidence remains fragmented. Some studies focus on the frequency and characteristics of ransomware attacks. Others examine emergency department utilization, ambulance operations, clinical outcomes, or the experiences of healthcare professionals. The studies ask related but different questions, so their findings cannot simply be combined into one severity measure. A further challenge is that publicly reported recovery milestones frequently emphasize the restoration of information technology systems rather than the return of clinical operations to normal or acceptable levels. A hospital may regain access to core applications while continuing to experience delayed care, manual reconciliation, or reduced throughput.

We therefore examine ransomware as an operational healthcare disruption rather than exclusively as an information security event. Our objectives are to:

- Synthesize empirical findings concerning the effects of ransomware attacks on healthcare service delivery.
- Identify measurable indicators of clinical and operational disruption.
- Distinguish technical restoration, operational recovery, and clinical recovery.
- Examine the extent to which ransomware-related disruption affects neighboring healthcare organizations and emergency medical services.
- Propose a structured framework for assessing disruption and recovery using operational evidence.

We do not try to establish a universal estimate of ransomware-related mortality, financial loss, or service downtime. Instead, we examine what the available studies show and where important gaps remain.

2 Review Approach and Scope

2.1 Review design

We use a critical narrative review approach. We draw on peer-reviewed empirical studies, qualitative investigations, health services research, relevant incident-response guidance, and healthcare cybersecurity policy materials. Our purpose is to identify recurring operational effects and assess which indicators are useful for evaluating clinical service disruption and recovery. The review does not constitute a systematic review or meta-analysis. No pooled effect size is calculated because the available studies differ substantially in research design, incident characteristics, settings, and outcome definitions.

2.2 Scope

We focus on ransomware incidents affecting hospitals and healthcare delivery organizations. We consider both direct disruption at attacked institutions and indirect effects on surrounding healthcare services. Relevant operational domains include hospital activity, emergency department performance, patient diversion, ambulance operations, clinical workflow continuity, patient outcomes, and recovery. Studies of cybersecurity incidents more broadly are considered where they provide relevant

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

methodological or operational insights, but findings are not automatically attributed to ransomware unless the underlying evidence supports that interpretation.

2.3 Evidence interpretation

The analysis distinguishes between observed operational changes, associations identified through statistical analysis, and causal conclusions supported by the study design. The difference is especially important when patient outcomes are discussed. Changes in mortality, length of stay, or treatment delays may be influenced by patient characteristics, seasonal demand, staffing, hospital capacity, and other concurrent events. For this reason, the review avoids treating every adverse outcome occurring during a ransomware incident as a demonstrated consequence of the attack.

2.4 Analytical approach

The literature is organized around five operational domains:

- Service availability.
- Patient flow and capacity.
- Clinical workflow continuity.
- Patient safety and outcomes.
- Recovery stability.

Together, the five domains form a practical framework for describing disruption and recovery. The framework is meant to guide research and operational monitoring; it is not a validated scoring instrument.

3 From Cybersecurity Compromise to Healthcare Service Disruption

3.1 The relationship between technical and clinical systems

Healthcare information systems support numerous activities that are essential to patient care. Electronic health records provide access to medical histories, clinical notes, medication lists, and diagnostic information. Laboratory and radiology systems support investigations and clinical decision-making. Scheduling and registration platforms coordinate patient movement and resource allocation. Communication systems enable coordination between clinical departments and external providers. When ransomware affects these systems, the consequences depend on which functions become unavailable, how long the interruption persists, and which contingency arrangements remain operational. A technical incident does not necessarily produce identical clinical effects across hospitals. Organizations differ in their digital architecture, staffing, service specialization, emergency preparedness, and ability to operate manually.

3.2 Direct and indirect disruption

Direct disruption occurs when an attacked organization loses access to systems or services necessary for its operations. Indirect disruption occurs when the incident affects other organizations or populations. For example, a hospital experiencing ransomware may divert ambulances to neighboring facilities. The receiving hospitals may then experience increased emergency department attendance, higher occupancy, or longer waiting times despite not being directly compromised. Dameff et al. [3] provide empirical evidence that a healthcare ransomware attack can generate measurable operational effects at adjacent emergency departments. The evidence shows why analysis should extend beyond the hospital that was attacked.

3.3 Operational degradation without complete shutdown

Clinical service disruption does not require complete hospital closure. A hospital may continue treating patients while experiencing reduced efficiency, delayed documentation, or limitations in diagnostic access. Manual procedures may preserve essential functions but increase staff workload and reduce

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

throughput. As a result, binary classifications such as operational versus non-operational may conceal important variation in service performance.

3.4 The importance of baseline performance

Operational indicators are most informative when compared with appropriate baseline conditions. An increase in emergency department waiting time may reflect ransomware-related disruption, but it may also result from ordinary demand fluctuations. Assessments should therefore account for historical patterns, comparable institutions, patient case mix, and other relevant contextual factors. Without such comparisons, operational changes may be incorrectly attributed to the cyberattack.

4 The WannaCry Attack as Evidence of Healthcare Operational Disruption

The 2017 WannaCry ransomware outbreak remains an important case in the study of healthcare cybersecurity because of its effects on National Health Service organizations in England. Ghafur et al. [1] examined the incident using available operational and financial information. Among infected hospitals, the study identified approximately 13,500 canceled outpatient appointments, 1,100 fewer emergency admissions, 2,200 fewer elective admissions, and 3,800 fewer emergency-department attendances during the attack week. The estimated value of lost activity at infected hospitals was £5.9 million; the analysis did not identify an increase in mortality [1]. The incident illustrates how a widespread cybersecurity event can interfere with healthcare delivery even where the consequences vary between affected organizations. WannaCry also demonstrates the limitations of assessing ransomware solely through the number of compromised computers.

The operational significance of an incident depends on the affected systems, the healthcare services that rely on them, and the availability of contingency arrangements. Yet the WannaCry incident is not representative of every healthcare ransomware attack. It involved a particular technical mechanism, historical context, and healthcare system structure. Its findings are therefore most useful for establishing the potential scale and diversity of operational consequences rather than predicting the effects of contemporary incidents. The broader lesson is that healthcare cyber incidents should be evaluated using service-delivery evidence alongside technical incident data.

5 Ransomware Incidence and the Measurement of Exposure

Neprash et al. [2] examined ransomware attacks affecting United States healthcare delivery organizations. Research of this kind contributes to understanding the frequency, distribution, and characteristics of reported incidents. Still, incident frequency and operational severity are different concepts. A count of ransomware attacks does not reveal how many patients experienced delayed care, how long clinical systems were unavailable, or whether neighboring institutions absorbed additional demand. Likewise, the number of affected records may describe the potential scale of a data breach without adequately representing disruption to healthcare delivery. Incident datasets may also depend on public reporting, regulatory disclosures, and the availability of reliable information about individual attacks. Incident databases, public reports, and regulatory records differ in both definition and completeness.

Operational research therefore requires more than identifying the occurrence of an attack. Where possible, incident records should be linked to healthcare utilization, hospital activity, staffing, patient outcomes, and recovery information. Such linkage enables researchers to investigate the relationship between cyber incidents and healthcare service performance.

6 Hospital Activity and Service Utilization

6.1 Hospital activity as an operational indicator

Hospital activity provides a potentially useful means of assessing ransomware-related disruption. Relevant measures include admissions, discharges, outpatient appointments, elective procedures,

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

emergency presentations, and diagnostic activity. Changes in these indicators may reveal reductions in service availability or shifts in patient demand. At the same time, their interpretation depends on the nature of the affected services. For example, a reduction in elective procedures may reflect a deliberate decision to prioritize emergency care rather than an inability to provide any clinical service.

6.2 Rural hospital disruption

Neprash et al. [4] investigated ransomware-related effects in rural hospital settings. During the initial attack week, inpatient admissions declined by an average of 14.7% at attacked rural hospitals and 16.9% at attacked urban hospitals. Inpatient volumes returned to statistically indistinguishable preattack levels by the second week for rural hospitals and the third week for urban hospitals [4]. Rural healthcare systems are particularly relevant because patients may have fewer nearby alternatives when a hospital experiences operational disruption. The consequences of reduced service availability can therefore depend on geography, referral arrangements, transport distances, and the capacity of surrounding institutions. Still, rural hospital findings cannot be generalized to large urban hospital networks. The availability of alternative facilities and the structure of healthcare delivery differ substantially between settings.

6.3 Interrupted versus displaced activity

A decline in activity at an attacked hospital does not necessarily mean that all corresponding care was forgone. Some patients may receive care at another institution. Others may experience delays, cancellation, or a change in treatment pathway. Canceled care and transferred care have different consequences. Researchers should distinguish between care that was permanently lost, care that was postponed, and care that was transferred elsewhere. Separating canceled from displaced activity helps show both the severity of the local disruption and the burden placed on nearby services.

6.4 Activity recovery

A return to pre-incident admission or procedure volumes may indicate operational normalization. Yet aggregate volume alone may conceal persistent backlogs or changes in case mix. Recovery assessments should therefore consider whether delayed activity has been resolved and whether the hospital can sustain normal operations without exceptional contingency arrangements.

7 Emergency Department Spillover and Regional Effects

7.1 Emergency department vulnerability

Emergency departments depend on timely patient assessment, diagnostic testing, clinical communication, and access to hospital capacity. When ransomware disrupts these functions, an attacked hospital may experience reduced throughput or need to divert incoming patients. The consequences can extend to surrounding emergency departments.

7.2 Evidence of spillover

Dameff et al. [3] examined emergency department activity associated with a ransomware attack on a nearby healthcare organization. At two unaffected emergency departments adjacent to four attacked hospitals, mean daily census increased by 15.1%, ambulance arrivals by 35.2%, median waiting-room time by 47.6%, and median length of stay for admitted patients by 33.9% during the attack-and-recovery period relative to the preattack period [3]. These are single-region before-and-after findings, but they demonstrate that cyber incidents can affect institutions beyond the directly attacked facility. Regional care can therefore deteriorate even when neighboring hospitals have not been technically compromised. A ransomware incident can therefore generate a form of operational interdependence in which the disruption of one institution changes demand and capacity elsewhere.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

7.3 Candidate operational indicators

Potential indicators of emergency department spillover include attendance volume, ambulance arrivals, waiting times, length of stay, patients leaving before completion of care, and boarding duration. No single pattern should be expected across all of these indicators. The effect depends on local hospital capacity, diversion policies, patient characteristics, and the duration of the incident.

7.4 Regional recovery

Regional recovery may occur later than technical restoration at the attacked hospital. Patients already diverted to other facilities, accumulated queues, and altered referral patterns may continue to affect surrounding institutions. A comprehensive recovery assessment should therefore consider both the attacked organization and the wider healthcare network.

8 Emergency Medical Services and Patient Transport

8.1 The role of emergency medical services

Emergency medical services (EMS) connect patients with hospital care. When a hospital becomes unavailable or restricts admissions, ambulance dispatch and transport decisions may change. Diversion may increase travel time, reduce ambulance availability, and shift patients to other hospitals.

8.2 Operational consequences

Potential EMS indicators include ambulance diversion frequency, transport duration, destination changes, handover delays, and resource availability. Still, changes in these measures should be interpreted within the relevant emergency response system. A longer transport time may reflect diversion, traffic conditions, geographic constraints, or differences in destination suitability.

8.3 Evidence from operations research

Arsalani et al. [7] address ransomware-related disruption and emergency medical services through an operations-research perspective. Using data from two ransomware incidents at major Alabama hospitals, they found that one incident substantially worsened three ambulance-performance measures while the other produced little or no effect; the difference was associated with the surrounding hospital network's capacity to absorb diverted patients [7]. The authors then used those empirical findings to construct a simulation framework for breach scenarios and mitigation options. The observed incident effects and the model-generated scenarios should be reported separately.

8.4 Implications for resilience

EMS resilience requires coordination between dispatch services, hospitals, and regional healthcare authorities. A hospital's recovery may remain operationally incomplete if ambulance routing restrictions continue or if the receiving network remains under unusual pressure.

9 Clinical Workflow Disruption and Manual Contingencies

9.1 Clinical dependence on digital workflows

Clinical work involves interdependent processes rather than isolated applications. A physician may need access to the electronic health record, medication history, laboratory results, imaging, and communication tools to complete a single episode of care. Disruption of one system can therefore affect several downstream activities.

9.2 Qualitative evidence

Van Boven et al. [5] investigated healthcare experiences associated with ransomware-related disruption. Qualitative studies can reveal difficulties that are not fully captured by routine activity data, including uncertainty, communication problems, workarounds, and changes in clinical decision-

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

making. The accounts show how healthcare workers keep services running under difficult conditions. At the same time, qualitative accounts do not independently establish the frequency or magnitude of particular operational outcomes across all healthcare organizations.

9.3 Manual documentation and workarounds

Manual procedures may enable essential care to continue when digital systems are unavailable. Examples include paper documentation, telephone communication, manual ordering, and temporary record-keeping arrangements. Such procedures can reduce immediate service interruption. Even so, they may also introduce additional work, slower information retrieval, transcription requirements, and subsequent reconciliation tasks. The existence of a workaround should therefore not be interpreted as evidence that service delivery is unaffected.

9.4 Workflow indicators

Potential measures include turnaround time for diagnostic requests, medication administration delays, documentation completion time, discharge processing time, and the proportion of workflows operating under contingency procedures. Each workflow indicator needs a clear definition. For example, a longer documentation time may reflect additional clinical complexity rather than ransomware-related inefficiency.

9.5 Post-restoration reconciliation

When digital systems return, organizations may need to transfer or reconcile information recorded during the outage. As a result, operational work may continue well after the systems are back online. The duration and consequences of such reconciliation should be evaluated rather than assumed.

10 Patient Safety and Clinical Outcomes

10.1 Distinguishing operational disruption from clinical harm

Operational disruption can create conditions that increase the risk of delayed or compromised care. Yet demonstrating actual clinical harm requires suitable outcome data and research methods. A canceled appointment or delayed diagnostic test is an operational consequence. Whether that delay caused a particular adverse clinical outcome is a separate question.

10.2 Evidence concerning service utilization and patient outcomes

Abouk and Powell [8] examined service utilization, not clinical outcomes. Across eight California ransomware attacks affecting 15 hospitals, emergency-department visits at attacked hospitals fell by 8.10% in the first week and 16.21% in the second week; inpatient admissions also declined, while nearby unattacked hospitals experienced a temporary increase in emergency-department visits [8]. These changes indicate displaced or deferred activity but do not, by themselves, establish patient harm.

Neprash, McGlave, and Nikpay linked ransomware incidents to Medicare claims and found that attacked hospitals' volumes declined by 17%–24% during the initial week and recovered within three weeks. Among patients already admitted when an attack began, the study estimated a 34%–38% increase in in-hospital mortality [6]. These estimates are consequential but should be interpreted within the study's population, design, and identifying assumptions rather than treated as a universal ransomware effect.

10.3 Critical care and clinical consequences

Pham et al. [9] examined 78 cardiac arrests at two untargeted hospitals adjacent to a ransomware-affected hospital system. Total cardiac arrests increased from 21 before the attack to 38 during it, and favorable neurological survival after out-of-hospital cardiac arrest decreased from 40.0% to 4.5%, returning to 41.2% after the attack period [9]. The study identified an association in a particular regional incident; it did not establish that ransomware universally produces the same cardiac-arrest

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

effects. Straw et al. [10] broadened the evidence base through a systematic review of 59 empirical case studies from 13 countries, supplemented by social-media narratives. They identified reported harms across multiple clinical groups, but the mixed source types and case-study evidence require care: the review maps reported harms and vulnerable groups rather than producing a single causal effect estimate [10].

10.4 Patient outcome indicators

Relevant measures may include mortality, complications, length of stay, readmission, treatment delays, and other condition-specific outcomes. Their suitability depends on the population and clinical pathway being investigated. Crude comparisons before and after an incident may be misleading if patient severity or service demand changes. Risk adjustment and appropriate comparison groups are therefore important.

10.5 Avoiding unsupported mortality claims

The available evidence does not justify assigning a universal number of deaths to healthcare ransomware incidents. Such estimates would require consistent definitions, complete incident data, appropriate comparison groups, and reliable attribution. Patient safety consequences should instead be reported according to the evidence available for each incident or study.

11 Technical Restoration, Operational Recovery, and Clinical Recovery

11.1 Technical restoration

Technical restoration refers to the recovery of affected information systems and infrastructure. Indicators may include system availability, restoration of network connectivity, recovery of applications, and the completion of technical containment activities. NIST contingency planning guidance [11] provides a foundation for understanding information-system recovery planning. Still, restoration of technical functionality is not necessarily equivalent to restoration of healthcare service performance.

11.2 Operational recovery

Operational recovery concerns the return of healthcare processes to acceptable or normal functioning. It may involve the resumption of routine appointments, diagnostic services, patient admissions, discharge processes, and electronic documentation. A hospital can be technically restored while continuing to operate below its usual capacity. Operational recovery should be measured using service-delivery indicators rather than technical milestones alone.

11.3 Clinical recovery

Clinical recovery concerns the resolution of patient-care consequences associated with the disruption. Clinical recovery may require staff to complete delayed investigations, manage postponed treatment, reconcile records, and review possible adverse outcomes. Not every clinical consequence can be reversed. As a result, clinical recovery should not be defined simply as a return to the pre-incident level of hospital activity.

11.4 Recovery as a multidimensional process

The three forms of recovery may occur at different times. Technical systems may return before normal patient throughput is restored. Clinical backlogs may persist after routine workflows resume. In some circumstances, manual procedures may maintain essential clinical activity while technical recovery remains incomplete. The relationship is therefore not a universally fixed sequence.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

11.5 Implications for incident reporting

Incident reports should identify which recovery milestone is being described. A statement that a hospital has recovered should specify whether it refers to technical systems, operational service levels, or the consequences for patients. Without this distinction, recovery reporting may overstate the extent to which healthcare delivery has normalized.

12 Critical Synthesis of Empirical Evidence

The literature demonstrates several recurring features of healthcare ransomware disruption. First, ransomware can interrupt healthcare delivery through the unavailability of information systems and associated workflows. Second, disruption can extend beyond the directly attacked institution. Third, operational consequences vary by hospital characteristics, affected systems, contingency capacity, and regional healthcare arrangements. Fourth, routine activity measures can provide evidence of disruption that is not captured by cybersecurity incident reports. Fifth, the restoration of technical systems does not establish that operational or clinical recovery has been completed. At the same time, the literature also contains important methodological differences. Studies of incident frequency measure exposure rather than service impact. Hospital utilization studies examine changes in activity but may not capture clinical quality.

Emergency department studies provide information about patient flow and regional spillover. Qualitative studies describe experiences and workflow adaptations. Patient outcome studies investigate possible clinical consequences but require careful causal interpretation. The methods complement one another, but they are not interchangeable.

Evidence area	Representative sources	Main contribution	Principal limitation
WannaCry disruption	Ghafur et al. [1]	Operational and financial consequences	Specific incident and healthcare system
Incident frequency	Neprash et al. [2]	Distribution of reported ransomware attacks	Does not directly measure clinical impact
Emergency department spillover	Dameff et al. [3]	Effects beyond the attacked institution	Context-dependent regional findings
Rural hospital activity	Neprash et al. [4]	Disruption in geographically constrained settings	Limited generalizability to other systems
Clinical workflow experiences	Van Boven et al. [5]	Workarounds and operational difficulties	Qualitative findings
Healthcare service effects	Neprash et al. [6]	Empirical assessment of ransomware consequences	Dependent on study population and measures
Emergency medical services	Arsalani et al. [7]	Network and transport-related consequences	Modeling or context-specific assumptions
Patient-level harms	Straw et al. [10]	Cross-specialty synthesis of reported harms and vulnerable groups	Heterogeneous case studies and social-media narratives
Service utilization and patient outcomes	Neprash et al. [6]; Abouk and Powell [8]; Pham et al. [9]	Hospital volume, regional displacement, and selected clinical outcomes	Study-specific populations, incidents, and causal assumptions
Organizational response	Ewoh and Vartiainen [12]	Healthcare ransomware challenges and responses	Review-level evidence

The combined evidence supports a multidimensional approach to operational monitoring. It does not support reducing all ransomware consequences to a single universally applicable severity score.

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

13 A Five-Domain Framework for Clinical Service Disruption and Recovery

13.1 Framework rationale

Existing incident reporting often emphasizes technical compromise, financial consequences, or system restoration. Technical measures matter, but they do not describe the full effect on healthcare delivery. The proposed framework identifies five domains that can be assessed separately.

13.2 Domain 1: Service availability

The service-availability domain asks whether essential care can still be delivered. Representative indicators include the availability of emergency care, outpatient services, elective procedures, diagnostics, and clinical information systems. The assessment should distinguish complete unavailability from reduced capacity.

13.3 Domain 2: Patient flow and capacity

The patient-flow domain tracks how people move through the healthcare system. Representative indicators include admissions, emergency department attendance, waiting time, length of stay, ambulance diversion, and hospital occupancy. Changes should be interpreted against suitable baselines and regional conditions.

13.4 Domain 3: Clinical workflow continuity

The workflow-continuity domain asks whether essential clinical work can continue safely and efficiently. Potential indicators include diagnostic turnaround times, documentation delays, medication workflow interruptions, and the use of manual contingency procedures. The assessment should consider both service continuation and the additional burden associated with workarounds.

13.5 Domain 4: Patient safety and outcomes

The patient-outcomes domain covers measurable consequences for patients. Indicators may include treatment delays, adverse events, complications, and risk-adjusted clinical outcomes. The selection of indicators should reflect the affected clinical services. Observed changes should not automatically be attributed to ransomware without appropriate evidence.

13.6 Domain 5: Recovery stability

The recovery-stability domain asks whether restored services can run consistently without special restrictions or repeated disruption. Indicators may include the duration of diversion arrangements, unresolved clinical backlogs, continued reliance on manual workflows, and repeated service interruptions. Recovery stability is particularly important because the first successful restoration of an application may not mark the end of operational disruption.

13.7 Framework summary

Domain	Principal question	Illustrative indicators
Service availability	Which healthcare services remain operational?	Canceled procedures, unavailable diagnostics, service restrictions
Patient flow and capacity	How is patient movement affected?	ED attendance, waiting times, admissions, diversion, length of stay
Clinical workflow continuity	Can essential care processes continue?	Manual procedures, diagnostic delays, documentation backlogs
Patient safety and outcomes	What consequences are observed for patients?	Treatment delays, complications, risk-adjusted outcomes

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

Domain	Principal question	Illustrative indicators
Recovery stability	Have services returned to sustainable functioning?	Persistent backlogs, repeated outages, continuing diversion

13.8 Interpretation of the framework

The domains should be evaluated in relation to the affected institution and its clinical context. Not every indicator will be relevant to every incident. For example, ambulance diversion may be central to a hospital emergency department but less informative for a specialist outpatient facility. The framework supports indicator selection rather than prescribing an identical measurement set for all organizations.

13.9 Why a composite score is not proposed

The reviewed studies do not establish validated weights for combining service availability, patient flow, workflow continuity, patient outcomes, and recovery stability. Assigning arbitrary weights could conceal clinically important differences. A hospital might restore normal admission volume while continuing to experience serious diagnostic delays. A single composite score could obscure this problem. The framework is intended for domain-level reporting until empirical validation supports more formal aggregation.

14 Illustrative Application to a Hospital Ransomware Incident

14.1 Scenario

Consider a hypothetical hospital that experiences a ransomware attack affecting electronic health records, scheduling, and selected diagnostic interfaces. Emergency care continues under contingency procedures, but elective appointments are postponed and ambulances are temporarily diverted. The scenario is illustrative and is not based on one reported incident.

14.2 Service availability

The hospital documents which services remain available and which are restricted. Rather than reporting only that the electronic health record is unavailable, the assessment identifies the specific clinical functions affected.

14.3 Patient flow and capacity

The hospital monitors emergency department arrivals, admission rates, waiting times, and ambulance diversion. Neighboring hospitals may also monitor changes in patient volume. That wider view captures both direct and regional disruption.

14.4 Workflow continuity

Clinical teams document the use of paper records, manual ordering, and alternative communication procedures. The assessment examines whether these arrangements maintain essential services and whether they introduce measurable delays.

14.5 Patient safety and outcomes

Relevant patient outcomes are monitored according to the affected services. Any observed adverse outcomes are investigated using appropriate clinical and epidemiological methods. They are not automatically attributed to the ransomware incident.

14.6 Recovery stability

After technical systems are restored, the hospital continues monitoring appointment backlogs, diagnostic turnaround times, diversion arrangements, and documentation reconciliation. Recovery is

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

considered operationally stable only when the relevant services have returned to acceptable functioning without continuing exceptional restrictions.

14.7 Value of the framework

The scenario illustrates how a multidimensional assessment can provide a more informative account of disruption than a single system-downtime figure. It also shows why technical restoration and clinical recovery should be reported separately.

15 Implications for Healthcare Cybersecurity and Resilience

15.1 Incorporating operational indicators into incident response

Healthcare cybersecurity response should include clinical service monitoring alongside technical containment and restoration. Relevant operational indicators should be identified before an incident occurs. Organizations can then compare the disruption with an established baseline.

15.2 Coordination between cybersecurity and clinical leadership

Technical teams may know when applications become available. Clinical leaders are better positioned to determine whether services can be delivered safely and efficiently. Recovery assessments therefore require coordination between cybersecurity, hospital operations, clinical departments, and emergency preparedness teams.

15.3 Regional coordination

The findings concerning emergency department spillover indicate that ransomware preparedness should not be confined to individual hospitals. Regional coordination may be necessary when patient diversion or service restrictions affect neighboring institutions. Emergency medical services should be included where hospital availability influences transport decisions.

15.4 Recovery planning

NIST contingency planning guidance [11] and the CISA StopRansomware Guide [13] provide relevant principles for incident preparation and technical recovery. Yet healthcare organizations must translate those principles into operational arrangements suited to clinical services. In practice, they must identify critical workflows, prepare fallback procedures, and define service-level recovery indicators.

15.5 Healthcare-specific cybersecurity objectives

The United States Department of Health and Human Services Healthcare and Public Health Cybersecurity Performance Goals [14] provide a healthcare-oriented foundation for cybersecurity improvement. The HHS goals provide a useful starting point for preparedness. Still, implementing cybersecurity controls does not by itself establish the effectiveness of clinical recovery. Operational monitoring and recovery exercises remain necessary.

15.6 Evaluating contingency procedures

Organizations should test whether manual procedures can sustain essential clinical activities. Exercises should consider documentation, diagnostic ordering, medication administration, communications, and patient transfer. The aim is not simply to confirm that a workaround exists, but to assess its operational limitations.

16 Research Gaps and Future Directions

16.1 Standardized disruption measures

The literature would benefit from standardized definitions of clinical service disruption. Different studies use different measures, making direct comparison difficult. Future research should examine

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

whether a common set of core indicators can be applied across healthcare systems while allowing local adaptation.

16.2 Longitudinal recovery measurement

More studies are needed that follow organizations beyond the initial restoration of technical systems. Such research could establish whether patient throughput, clinical workflows, and service quality return to baseline at different times.

16.3 Regional spillover

Research should examine the extent to which ransomware attacks affect neighboring hospitals, emergency medical services, and referral networks. The magnitude of these effects may depend on geographic isolation, hospital capacity, and regional coordination.

16.4 Clinical outcomes

Further research is needed to assess patient outcomes using appropriate comparison groups and risk adjustment. Particular attention should be given to distinguishing direct clinical effects from changes caused by patient diversion or differences in case mix.

16.5 Contingency effectiveness

The effectiveness of manual workflows and alternative service arrangements requires systematic evaluation. Studies should examine not only whether care continues, but also the resulting workload, delays, and potential safety implications.

16.6 Framework validation

The proposed five-domain framework requires empirical evaluation. Future research should test its completeness, feasibility, and usefulness in both retrospective incident analysis and prospective preparedness exercises.

17 Discussion

Healthcare ransomware attacks create operational risks because clinical services depend on interconnected digital infrastructure. The consequences of an attack are therefore shaped by the relationship between technical system availability and healthcare delivery. Published evidence shows that ransomware can disrupt hospital activity, emergency departments, clinical workflows, and, in some settings, patient outcomes. The WannaCry study by Ghafur et al. [1] provides evidence of substantial service disruption within a national healthcare system. Research on ransomware incidence [2] demonstrates the importance of understanding the distribution of attacks, although incident counts alone cannot describe their clinical consequences. Dameff et al. [3] demonstrate that disruption may extend beyond the directly attacked organization. Regional links between emergency services and hospital capacity make spillover especially important.

Research involving rural hospitals [4] further indicates the need to consider local healthcare geography and the availability of alternative services. Qualitative evidence [5] adds an important perspective by examining how healthcare workers respond when normal digital workflows become unavailable. Such studies reveal operational burdens that may not be visible in administrative datasets. Studies addressing clinical outcomes [8,9] extend the analysis beyond service activity, but they also highlight the importance of careful causal interpretation. The principal analytical problem is that different forms of disruption are often treated as equivalent. Technical downtime, reduced service volume, patient diversion, workflow delays, and adverse clinical outcomes describe different phenomena. They may be related, but they should not be combined without a clear methodological justification.

The distinction between technical restoration, operational recovery, and clinical recovery is therefore central to the proposed approach. Restoring an electronic health record system may be necessary for recovery, but it does not establish that delayed appointments have been completed or that clinical

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

documentation backlogs have been resolved. Likewise, continued patient care during a technical outage does not establish that operations are functioning at their normal level. The proposed five-domain framework provides a means of organizing these differences. Service availability identifies which functions remain operational. Patient flow and capacity describe changes in demand and throughput. Clinical workflow continuity addresses the ability to maintain essential care processes. Patient safety and outcomes concern the consequences for patients. Recovery stability examines whether restored services can operate sustainably.

Together, these domains provide a more complete representation of healthcare ransomware disruption than technical indicators alone. Still, the framework remains conceptual and is not a validated measure of organizational resilience. Its contribution is to clarify which dimensions should be examined and to support more transparent reporting of operational consequences.

18 Limitations

Several limitations should be noted. First, it adopts a critical narrative approach rather than a systematic review methodology. Second, the empirical literature includes studies with different designs, populations, and operational measures. Third, incident characteristics vary substantially, limiting the generalizability of findings from individual ransomware events. Fourth, public incident reporting may be incomplete and may not consistently document operational consequences. Fifth, changes in hospital activity can be influenced by factors unrelated to ransomware, including staffing, demand, seasonal variation, and patient case mix. Sixth, qualitative and modeling studies provide important insights but cannot always establish the magnitude of effects observed in routine clinical practice. Seventh, the proposed framework has not been empirically validated.

Finally, the review does not establish a universal relationship between ransomware attacks and patient mortality. Such conclusions require incident-specific evidence and appropriate analytical methods.

19 Conclusion

Ransomware attacks against healthcare organizations should be understood as potential disruptions to clinical service delivery rather than exclusively as information security incidents. The available literature demonstrates that their consequences may include reduced hospital activity, altered emergency department demand, ambulance diversion, interrupted clinical workflows, and possible adverse patient outcomes. At the same time, these effects vary between incidents and healthcare settings. Technical system downtime does not provide a complete measure of operational disruption, and technical restoration does not establish that clinical services have fully recovered. We propose a five-domain framework encompassing service availability, patient flow and capacity, clinical workflow continuity, patient safety and outcomes, and recovery stability.

The framework offers a structured way to describe ransomware consequences while separating observed effects from claims that still need evidence. Future research should prioritize standardized operational indicators, longitudinal recovery studies, regional spillover analysis, and rigorous evaluation of clinical outcomes. Healthcare ransomware resilience ultimately requires not only the ability to restore information systems, but also the capacity to sustain and recover essential patient care.

REFERENCES

[1] Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digital Medicine, 2, 98. https://doi.org/10.1038/s41746-019-0161-6

[2] Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. JAMA Health Forum, 3(12), e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

[3] Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., Hemmen, T. M., Clay, B. J., & Longhurst, C. A. (2023). Ransomware attack associated with disruptions at adjacent

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)

emergency departments in the US. JAMA Network Open, 6(5), e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270

[4] Neprash, H. T., McGlave, C. C., Rydberg, K., & Henning-Smith, C. (2024). What happens to rural hospitals during a ransomware attack? Evidence from Medicare data. The Journal of Rural Health, 40(4), 728–737. https://doi.org/10.1111/jrh.12834

[5] 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. (2024). Hacking acute care: A qualitative study on the health care impacts of ransomware attacks against hospitals. Annals of Emergency Medicine, 83(1), 46–56. https://doi.org/10.1016/j.annemergmed.2023.04.025

[6] Neprash, H. T., McGlave, C. C., & Nikpay, S. S. (2026). Hacked to pieces? The effects of ransomware attacks on hospitals and patients. American Economic Journal: Economic Policy, 18(1), 256–281. https://doi.org/10.1257/pol.20240594

[7] Arsalani, P., Dayarian, I., Freeman, N., Kim, Y., Peng, D., Zhao, M., Gray, J., & Crawford, W. (2026). Impact of ransomware on emergency medical services: Empirical estimation and risk assessment framework. Omega, 143, 103578. https://doi.org/10.1016/j.omega.2026.103578

[8] Abouk, R., & Powell, D. (2024). Ransomware attacks, ED visits and inpatient admissions in targeted and nearby hospitals. JAMA, 331(24), 2129–2131. https://doi.org/10.1001/jama.2024.7752

[9] Pham, T. T., Loo, T. M., Malhotra, A., Longhurst, C. A., Hylton, D., Dameff, C., Tully, J., Wardi, G., Sell, R. E., & Pearce, A. K. (2024). Ransomware cyberattack associated with cardiac arrest incidence and outcomes at untargeted, adjacent hospitals. Critical Care Explorations, 6(4), e1079. https://doi.org/10.1097/CCE.0000000000001079

[10] Straw, I., Kumar, D., Kweon, S., Selzer, J., Dameff, C., & Tully, J. (2026). Unveiling patient-level harms and at-risk clinical groups during hospital cyberattacks: Systematic review of global case studies and social media data. Journal of Medical Internet Research, 28, e88257. https://doi.org/10.2196/88257

[11] Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34 Revision 1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-34r1

[12] Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. Journal of Medical Internet Research, 26, e46904. https://doi.org/10.2196/46904

[13] Cybersecurity and Infrastructure Security Agency. (2023). #StopRansomware Guide. U.S. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/stopransomware/ransomware-guide

[14] U.S. Department of Health and Human Services. (2023). Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals. https://hhscyber.hhs.gov/documents/cybersecurity-performance-goals.pdf

© 2026 The Author(s) | Published by - Scholiora Research Publications
Creative Commons Attribution 4.0 International License (CC BY 4.0)