International Journal of Computers and Informatics (IJCI)

IJCI

المجلة الدولية للحاسبات والمعلوماتية

Vol. (5), No. (2)

February 2026

الإصدار (5)، العدد (2)

A Consideration of Potential Strategies for Patient Safety from Cyberattack in the Healthcare Domain

Noora Alallaq
Department of Computer Networks, College of Computing and informatics,
University of Al-Hamdaniya, Iraq
noora@uohamdaniya.edu.iq

Murthad Hussein Al-Yoonus
Department of Computer Networks, College of Computing and informatics,
University of Al-Hamdaniya, Iraq
Murthad.sabre@uohamdaniya.edu.iq

Muhmmad Al-Khiza'ay
Department of Computer Networks, College of Computing and informatics,
University of Al-Hamdaniya, Iraq
mak@uohamdaniya.edu.iq

Baobao Song
University of Technology Sydney, Australia
baobao.song@student.uts.edu.au

Abstract

The rapidly rising convergence of digital solutions in healthcare has enhanced performance and patient care, but introduced numerous cybersecurity challenges. Cyberattacks of all types—including ransomware, phishing, and supply chain intrusions—have grown in frequency and severity, focusing clearly on sensitive health data and disrupting essential clinical services. These events may result in the delay of the treatment, and the Inaccuracy of care, and at times, even put lives of patients in danger. This review considers healthcare cyber threats and analyses the effects of these threats, whether direct or circumstantial, on patient safety. It proposes an integrated approach that includes technical, managerial, and governance measures proactively prevent, reduce, and recover from cyber events. Some of the primary measures include proper network partitioning, real-time monitoring of system threats, comprehensive training for employees, incident response strategies, and increased control from regulators. By shifting the approach to cybersecurity as a matter of

https://doi.org/10.59992/IJCI.2026.v5n2p4
E-ISSN 2976-9361

patient safety, rather than just an IT problem, hospitals can improve their ability to counter cyber risks and sustain the delivery of safe and high-quality services. This review supports a multi-disciplinary strategy to incorporate cybersecurity into safety culture and operational strategy at the clinical level.

Keywords: Cybersecurity, Health Care Safety, Potential Threats, Information Security.

1. Introduction

The use of cloud-based systems, telemedicine, connected medical devices, and electronic health records (EHRs) is propelling the healthcare sector's rapid digital transformation. These developments have improved accessibility, improved patient outcomes, and maximized operational effectiveness. Healthcare is one of the industries most frequently targeted by cyberattacks, though, because of the new vulnerabilities brought about by this technological integration [10]. Healthcare organizations are especially vulnerable to cyberattacks because of the sensitive nature of medical data and the pressing need for system availability.

Beyond monetary loss and data breaches, cyberattacks in the healthcare industry have other repercussions. Attacks like ransomware have the potential to stop hospital operations, postpone medical care, and even kill patients because of corrupted data or system failures [13, 21]. Over 80 hospital trusts have affected by the 2017 WannaCry attack on the UK's National Health Service, which resulted in cancelled surgeries and emergency care being diverted [11]. Ransomware attacks in the United States have recently compelled providers to switch back to manual procedures, which a substantial negative influence clinical efficiency and raised the possibility of medical errors [15].

The complexity of healthcare workflows, inadequate cybersecurity investment, outdated IT systems, and a lack of employee training are some of the factors that make the healthcare industry vulnerable. Even though laws like HIPAA and GDPR require patient data to protected, cybersecurity maturity is not the same as compliance [8]. Furthermore, many organizations do not have a single strategy that ties IT security to clinical continuity and patient safety. This disparity emphasizes the necessity of an all-encompassing approach that considers cybersecurity to be a fundamental patient safety concern.

Clinical safety frameworks must integrated with cyber defence. Resilience can increased through techniques like medical device hardening, regular simulation-based incident response drills, security risk assessments, and Zero Trust Architecture [14]. Embedding cybersecurity awareness in clinical training and governance, builds an immune system to thwart most common breaches and speed recovery following a cyber-incident. Pragmatic cybersecurity within health would therefore, be proactive, patient focused and operational, within both technical and clinical domains.

In this review, we also discuss the changing threat landscape in the field of cybersecurity within healthcare and present novel approaches that prioritize patient safety.

2. Related Work

For the past decade, there has been an increased focus on the crossover between cybersecurity and healthcare. The wide range of research dealing with technical issues, organizational readiness, and even dealing with regulatory issues evidences this. Most literature attempts to describe and catalog the cyber threats targeting healthcare systems. Alarmingly, there is no uniform security protocol at healthcare organizations, which [14] considers one of the more common threats- ransomware, phishing, and insider breaches. [17] Also explored vulnerabilities found in electronic health records (EHR) which highlighted the need for tighter access control, stronger encryption, and better overall access management.

Some literature discusses the cyberattacks targeting healthcare systems from an operational and economic perspective. The healthcare sector incurs the most expensive data breaches of any sector according to the [18]. In addition, victims of these breaches suffer from loss of trust and prolonged recovery times. [16] Remarked that critical healthcare infrastructure has lagged behind in investment-suffering cyber security spending, which exacerbates the vulnerable state of the infrastructure.

The clinical ramifications of cyber incidents have gained more attention in recent years. [19] talked about how system outages, especially during ransomware attacks, can delay diagnosis and treatment. They discovered that system outages raised the possibility of workflow interruptions and medical errors. Similar to this, [21] suggested that cybersecurity incidents ought to seen as latent safety risks that could jeopardize patient outcomes rather than merely being IT problems.

Few studies have put forth integrated strategic frameworks that match cybersecurity practices with patient safety objectives, despite the fact that the body of research on the subject is expanding [1]. Current research frequently treats technical solutions (such as firewalls, antivirus software, and network segmentation) independently of human factors and clinical procedures.

Furthermore, although simulation-based training is widely used in clinical education, its application in cybersecurity readiness is still relatively new [9].

By providing a thorough analysis of healthcare cyber-threats from the standpoint of patient safety, this paper expands on earlier research. It offers a cohesive, patient-centered cybersecurity strategy by combining knowledge from the technical, organizational, and clinical domains.

3. Problem View

Healthcare organizations' significant reliance on digital infrastructure, sensitive patient data, and frequently insufficient cybersecurity protocols make them prime targets for cyberattacks. Healthcare systems increase their digital footprint and, consequently, their vulnerability to cyber threats as they embrace cloud-based services, telemedicine platforms, electronic health records (EHRs), and connected medical devices (IoMT).

The ramifications of cybersecurity breaches in the healthcare industry go beyond data loss or monetary loss, in contrast to cyberattacks in other industries. In clinical settings, patient care, diagnosis, treatment, and results has directly influenced by the confidentiality, availability, and integrity of health information.

A cyberattack that takes down a hospital's network can cause delays in life-saving patient records, interfere with the delivery of medications, or postpone urgent surgeries. As a result, these incidents present immediate and serious risks to patient safety in addition to IT difficulties.

Recent high-profile ransomware attacks have illustrated the disastrous effects of cyber disruptions, as evidenced by the WannaCry-infected NHS hospitals in the UK (2017) and the UHS hospital system in the U.S. (2020). Appointments has cancelled, ambulances has diverted, surgeries has delayed, and electronic communications has completely stopped because of these incidents. According to [19], some research has even connected cybersecurity incidents to higher death rates, particularly when they cause delays in treatments that are necessary right away.

3.1 Key Obstacles Found:

- System faults cause delays in emergency treatment.
- Disturbance of tools for diagnosis and medical devices.
- Changes in patient records, either loss or manipulation
- Clinical teams' scattered accountability for IT.
- Undervaluation of patient suffering in risk analyses.
    - Introduce a **risk quantification model** for patient safety under cyberattacks.
    - Example: Define a Cyber-Patient Risk Index (CPRI):

$$CPRI = \alpha \cdot P_a + \beta \cdot I_d + \gamma \cdot C_c$$

where:
P_a = probability of attack occurrence
I_d = expected downtime impact (hours × number of patients affected)
C_c = clinical consequence severity score (0–1 scale)
α, β, γ = weight coefficients determined via expert elicitation
→ This provides a measurable way to compare risks across hospitals.

3.2 Key Obstacles Found:

- System faults cause delays in emergency treatment.
- Disturbance of tools for diagnosis and medical devices.
- Changes in patient records, either loss or manipulation
- Clinical teams' scattered accountability for IT.
- Undervaluation of patient suffering in risk analyses.

3.3 Current Situation of Cyber Threats in Health Care Viruses and malware:

Because they depend on continuous access to electronic health records (EHRs), hospitals especially run the risk of ransomware. Recent strikes have resulted in postponed operations, rerouting of emergency services, and large financial losses.

3.4 Phishing and Credential theft:

Campaigns of targeted phishing prey on human mistake. Personal health information (PHI) breaches sometimes follow from staff account compromise.

3.5 Vendor Risk and Supply Chain:

Third-party services are quite important for healthcare systems, many of which lack strong security measures. Widespread data compromise has resulted from breaches through vendor systems.

3.6 Insider Threats:

Staff members' intentional or careless behavior accounts for a significant amount of data breaches. Two still major gaps are security awareness and access restrictions.

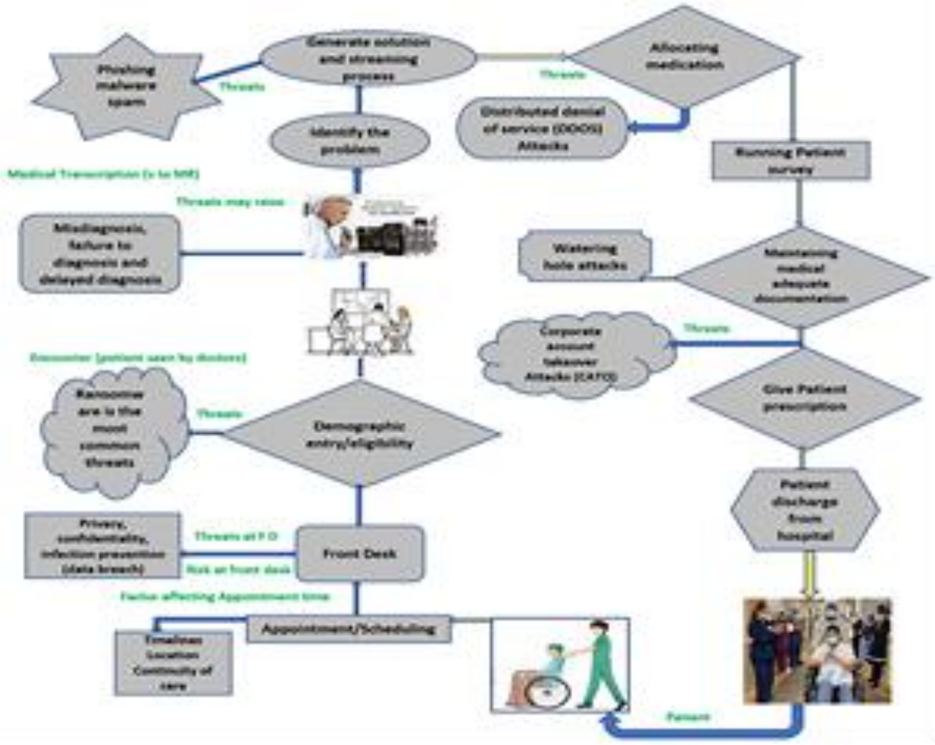
Phishing malware spam
Threats
Generate solution and streaming process
Threats
Allocating medication
Distributed denial of service (DDOS) Attacks
Identify the problem
Running Patient survey
Medical Transcription (s to MR)
Threats may raise
Misdiagnosis, failure to diagnosis and delayed diagnosis
Watering hole attacks
Maintaining medical adequate documentation
Corporate account takeover Attacks (CATO)
Threats
Encounter (patient seen by doctors)
Ransomw are is the most common threats
Threats
Demographic entry/eligibility
Give Patient prescription
Patient discharge from hospital
Privacy, confidentiality, infection prevention (data breach)
Threats at F D
Risk at front desk
Front Desk
Factor affecting Appointment time
Appointment/Scheduling
Timeliness Location Continuity of care
Patient

Figure 1. Visualizes the chain from cyberattack to patient harm

4. Implications for Patient Safety

Will insert a **mathematical reliability model** to capture downtime effect on care as showing in figure 2.

$$R(t) = e^{-\lambda t}$$

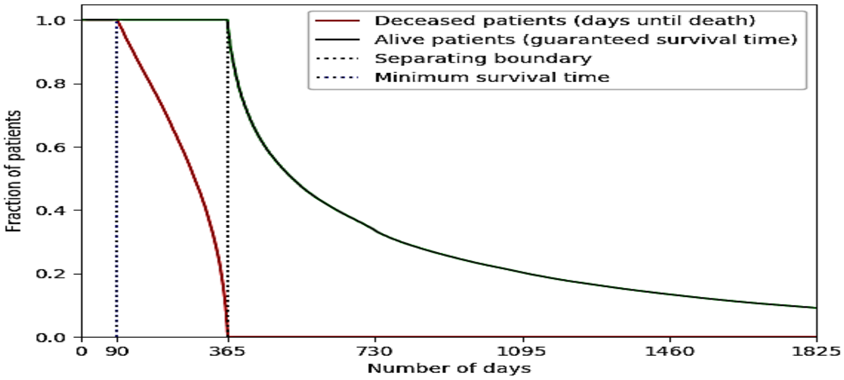

Figure (2). Reliability Model Graph

Where:

$R(t)$ is system reliability, and λ is the failure rate (e.g., ransomware events per year).

Link decrease in $R(t)$ to probability of delayed treatment.

Even though cybersecurity incidents has frequently presented as risks to money or reputation, it is becoming more and clearer how they affect patient care:

Table (1). Examples of hospitals exposed to cyberattacks

Hospital / Health System	Targeted System / Region	Year	Cyberattack Category	Result	Publication Source
HGO Hospital, Portugal	Internal hospital network (Lisbon)	2023	Ransomware	21-day disruption; €90M+ financial losses; transition to manual processes	[7]
Health Service Executive (HSE), Ireland	National Health IT network	2021	Ransomware	80% of IT systems affected; cancer treatments delayed; €100M+ estimated cost	[2]
Brno University Hospital, Czech Republic	COVID-19 testing and medical systems	2020	Ransomware	Operations shut down; surgeries delayed during peak of COVID-19 pandemic	[4]
Düsseldorf University Hospital, Germany	IT systems including patient files	2020	Ransomware	Hospital shutdown; one patient death due to rerouting; legal investigation	[5]
U.S. Hospitals (Surveyed)	National survey across regions	2019–22	Ransomware & Phishing	Increased ransomware; associated delays in EHR access and clinical diagnostics	[5]
SingHealth, Singapore	Centralized health data servers	2018	Data breach (APT)	1.5 million patient records accessed; failure in patching and security training	[6]

4.1. Clinical Delays:

Treatment and communication have delayed when EHRs and diagnostic systems are unavailable.

4.2 Compromise of Care:

Inaccurate or unavailable data may result in misdiagnosis, medication errors, or surgeries performed at the incorrect location.

4.3 Operational Disruption:

Clinical teams are strained and patient throughput has decreased when scheduling or monitoring systems are unavailable.

4.4 Psychosocial Harm:

When private patient information has compromised, it can lead to distress, particularly in cases involving mental health or stigmatized conditions.

5. Framework for Cyber-Resilient Patient Safety Strategy

This section describes a multi-layered strategy that combines patient safety objectives with cybersecurity:

- Add an **optimization model** for resource allocation:

$$\max U = \sum_{i=1}^{n} w_i \cdot S_i$$

subject to budget B:

$$\sum_{i=1}^{n} c_i \leq B$$

where:

S_i = safety improvement score from control i (training, backup, ZTA, etc.)
c_i = cost of control i
w_i = weight based on patient outcome importance.

→ shows a rational way to choose interventions.

5.1. Using technical controls to prevent:

- Put multi-factor authentication and zero-trust architectures into practice.
- Segment networks to separate administrative tasks from clinical systems.

5.2. Organizational Readiness:

- Provide staff training that emphasize social engineering awareness and cyber hygiene.

- Include cybersecurity simulations in emergency preparedness initiatives for hospitals.
- Create protocols for downtime that incorporate clinical workarounds.

5.3. Continuity and Incident Response:

- Keep your communication and incident response plans up to date.
- Test backup systems and recovery time goals on a regular basis.
- The restoration of mission-critical clinical systems should give top priority.

5.4. Compliance and Governance:

Integrate cybersecurity into systems for quality control and risk management.

- Create metrics and oversight for cyber resilience at the board level.
- Comply with laws like NIST CSF, GDPR, and HIPAA.

The following list show numerous techniques for handling cyberattacks in the healthcare industry with an emphasis on patient safety as showing in table (2).

Table (2): techniques for handling cyberattacks in the healthcare industry

Classification	Strategy	An explanation	Anticipated Effect on Patient Safety
Technical	Advanced Threat Detection & Response (EDR, SIEM, AI)	Use AI-powered solutions to instantly identify insider threats, malware activity, and anomalies.	Clinical workflow disruptions are avoided through early threat identification.
	Network Segmentation and Microsegmentation	Keep patient data systems and vital medical equipment separate from other network traffic.	Protects mission-critical systems during breaches and restricts the spread of attacks.
	Zero Trust Architecture (ZTA)	Apply "never trust, always verify" principle across all users and devices.	Reduces lateral movement of attackers and prevents unauthorized access to patient data.
	Immutable Backups and Offline Data Vaulting	Keep safe offline backups of patient data and configurations that are impenetrable.	Guarantees care continuity and recovery in the event of ransomware attacks.
Clinical	Downtime Procedure Simulation & Failover Protocols	Create and practice manual workarounds for outages in the lab, pharmacy, and EHR systems.	Maintains the provision of care in the event of cyber disruptions.

	Clinical-Cyber Incident Response Team (CCIRT)	To respond to cyber incidents in a coordinated manner, form teams of clinicians and IT security specialists.	Guarantees that patient-Impacting systems are prioritized in real time.
	Safety-Centered Risk Assessment for Medical Devices (IoMT)	Examine medical devices for possible patient cyber-safety hazards in addition to compliance. (e.g., improper dosage from pumps that have been compromised)	Protects against damage from compromised device functions.
Organizational	Governance of Cybersecurity Clinical Governance Integration	Include cyber risk as a regular topic on executive oversight committees and hospital safety boards.	Focuses on patient outcomes rather than just compliance when it comes to cybersecurity.
	Continuous Workforce Cyber-Awareness Training (Role-Based)	Provide role-specific threat scenarios in training for technical teams, administrative personnel, and clinicians.	Lowers the risk of insider threats, phishing success, and human error.
	Incident Command System (ICS) for Cyber Disruptions	Utilize disaster preparedness models, such as FEMA ICS, to organize and coordinate departmental responses to cyber incidents.	Enhances crisis response's prioritization of safety, accountability, and communication.
Policy & External	Cybersecurity Maturity Assessments (e.g., NIST CSF, HITRUST)	Assess cyber readiness by third parties using industry standards.	Finds security flaws that directly affect the continuity of patient services.
	Cyber Insurance with Patient Safety Clauses	Make use of policy incentives linked to incident transparency and patient harm reduction.	Encourages responsible response and preparation practices.
	National Health-CERT Participation & Intelligence Sharing	Engage in threat intelligence sharing networks tailored to the health sector.	Allows for the quicker mitigation of new risks that could jeopardize patient care.
	Vendor Risk and Supply Chain Cybersecurity Compliance	Demand that outside partners adhere to strict cybersecurity guidelines for the health sector (e.g., SOC 2, ISO 27001).	Avoids indirect risks from cloud providers, billing systems, and third-party software.

6. Future work

Future cybersecurity research and innovation must advance to meet new challenges while putting patient safety first as healthcare systems continue to digitize. This review identifies a number of important areas for further research:

6.1. Creation of Frameworks for Patient-Centric:

Few cybersecurity models currently in use in the healthcare industry specifically address how cyber threats affect clinical workflows and patient outcomes; instead, they concentrate on data protection and system resilience. Future studies should concentrate on creating integrated frameworks that integrate clinical risk assessments into cyber risk models and match cybersecurity planning with patient safety goals.

6.2. Clinical Impact Analysis and Real-Time Threat Detection:

Advanced real-time detection systems are required that can anticipate the clinical repercussions of cybersecurity breaches in addition to identifying them. The integration of AI-driven monitoring tools that evaluate in real time how a cyberattack impacts patient access to care, diagnostics, or treatment continuity should be investigated in future research.

6.3. Clinical Staff Cybersecurity Training One of the main reasons for cyber breaches is still human error:

The effectiveness and design of simulation-based cybersecurity training for healthcare professionals—rather than just IT staff—should investigated in future projects. Hospital accreditation requirements and continuing medical education should incorporate this kind of training.

6.4. Protocols for Downtime and Resilience Planning:

Few institutions have thorough clinical downtime protocols that been tested in real-world scenarios, despite the fact that many have backup systems. In order to guarantee patient safety during extended IT outages, future research should concentrate on developing, assessing, and standardizing such protocols.

6.5. Research on Ethics and Regulation:

Regulatory frameworks need to change as third-party technologies, remote care platforms, and cross-border data exchanges become more common. Future studies should look into the legal and ethical frameworks that regulate governments, healthcare providers, and vendors' obligations in cybersecurity, particularly in times of emergency.

6.6. Extended Research on Patient Results Following Cyberattack:

The long-term effects of cyberattacks on patient health outcomes, like delayed diagnoses, readmissions, or mortality, hardly been quantitatively assessed in research. Future longitudinal research should planned to evaluate the long-term effects of cyber incidents on particular clinical indicators.

6.7. Emerging Technologies and Cybersecurity:

Future research must evaluate the risks posed by IoMT (Internet of Medical Things), cloud computing, blockchain, and AI-assisted diagnostics, and develop strong defenses that do not jeopardize patient safety or care effectiveness.

7. Recommendations

Given the review's conclusions, a number of tactical suggestions are put forth to fortify healthcare systems against cyberattacks and guarantee that patient safety always takes precedence in cybersecurity preparation and reaction.

7.1 Integrate Cybersecurity into Frameworks for Patient Safety:

Cybersecurity is no longer just an IT or compliance problem. Cybersecurity risk must formally incorporated into patient safety governance frameworks in healthcare organizations. Including cyber risk assessments in clinical risk assessments is one example of this.

Reporting cyber incidents via the same channels as near misses and medical errors.

- Forming collaborative cybersecurity safety committees between IT and clinical.

7.2. Adopt Organization-Wide Cyber Resilience Training Regular cybersecurity:

Training that is specific to healthcare settings should provide to all healthcare staff, clinical and non-clinical. Included in the training should be:

- Phishing exercise simulations.
- Rehearsals of the downtime protocol.
- Knowledge of how assaults can jeopardize patients and interfere with the provision of care.
- Create and evaluate protocols for incident response and downtime.

Healthcare companies need to create thorough plans for responding to cyber incidents and downtime, and they should test them frequently.

7.3. Use cutting-edge technologies for threat detection and response:

Healthcare providers should implement the following:

- Intrusion detection systems (IDS).
- Tools for endpoint detection and response (EDR).
- Threat analytics based on artificial intelligence.

These tools can stop ransomware or other harmful activity from spreading and spot suspicious activity early.

7.4. Implement Supply Chain and Vendor Security Guidelines:

- Strict security regulations must applied to third-party vendors.
- Data protection provisions should be included in contracts.
- Timelines for mandatory breach notifications.
- Assessments of vendor risk ought to be a standard component of procurement.

7.5. Encourage cooperation and information exchange:

Participation in regional and national cybersecurity information-sharing networks, like the Health Information Sharing and Analysis Center (H-ISAC), has recommended for health systems.

- Coalitions for Regional Health Cybersecurity.

Collaborative reporting strengthens collective defense and aids in the early detection of attack patterns.

7.6. Encourage the Improvement of Policies and Regulations Legislators ought to:

- Make it mandatory to report cyber incidents involving healthcare.
- Establish minimal cybersecurity requirements for both public and private healthcare organizations.
- Synchronize health-specific laws (like HIPAA) with the realities of today's cyber threats. The worldwide scope of cybercrime targeting the healthcare industry necessitates international collaboration as well.

These suggestions seek to improve the cyber resilience of the healthcare industry while prioritizing patient safety in all security initiatives.

8. Conclusion

The risk of cyberattacks on healthcare systems is increasing, compromising patient safety and well-being, as well as data breaches. With the healthcare sector's heavy reliance on digital infrastructure, the impacts of cybersecurity breaches—including exam compromise, missed appointments, and loss of vital data—can have a direct impact on patient outcomes. Rather than framing cybersecurity as a technical or IT problem, emphasizing the importance of cyber as a fundamental component of providing safe, high-quality healthcare. This research underscores the need for a proactive and comprehensive cybersecurity strategy to protect patient data. It is important to adopt approaches that include incident response preparation, comprehensive staff training, instilling a culture of cybersecurity awareness, and purchasing robust security equipment. By integrating cybersecurity into patient safety frameworks, healthcare organizations can support risk mitigation, maintain trust in digital health systems, and ensure continuity of care.

Reference

[1] Birk, S., Clark, M., & Stensland, J. (2023). Association of ransomware attacks with delays in care and patient outcomes in US hospitals. JAMA Network Open, 6(2), e225425.

[2] Clarke, M., O'Reilly, M., & Smith, P. (2022). Lessons from the 2021 HSE ransomware attack: Implications for health service resilience. BMJ Global Health, 7(6), e009921.

[3] Gharib, R. K., Khalil, A., & Alkass, S. (2022). The Düsseldorf University Hospital ransomware incident: Implications for patient safety. Digital Health, 8, 20552076221104665.

[4] Haslinger, L., & Koska, S. (2021). Brno University Hospital ransomware attack during COVID-19: A wake-up call. Journal of Medical Internet Research, 23(4), e21747.

[5] Johnson, C., Grube, M., & Ellis, R. (2022). Cybersecurity incidents in U.S. hospitals: Survey results from 2019 to 2021. JAMA Health Forum, 3(6), e221126.

[6] Kaur, R., & Kaur, P. (2020). Analyzing the SingHealth breach: A Singaporean perspective on health data security. Health Informatics Journal, 26(4), 2730–2743.

[7] Morgado, L., Costa, M., & Vasconcelos, A. (2023). Cyberattack at Hospital Garcia de Orta (Portugal): A digital health system at risk. JMIR Formative Research, 7, e41738.

[8] Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. International Journal of Internet and Enterprise Management, 6(4), 279–314.

[9] Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. Journal of Medical Systems, 43(1), 7.

[10] Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52.

[11] Department of Health and Social Care. (2018). Lessons learned review of the WannaCry ransomware cyber-attack.

[12] Johnson, C., Badovinac, K., & Hayden, J. (2021). Cybersecurity: A latent threat to patient safety. BMJ Health & Care Informatics, 28(1), e100298.

[13] Koppel, R., Smith, S., Blythe, J., & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: You want my password or a dead patient? Studies in Health Technology and Informatics, 208, 215–220.

[14] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1–10.

[15] Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? BMJ, 358, j3179.

[16] Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2021). Cybersecurity and healthcare: How safe are we? BMJ, 372, n71.

[17] McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, 108, 57–68.

[18] Ponemon Institute. (2022). Cost of a Data Breach Report 2022. IBM Security.

[19] Singh, R., Sittig, D. F., & Classen, D. C. (2022). The safety implications of electronic health records downtime: A review. JAMA Health Forum, 3(7), e222257.

[20] U.S. Department of Health and Human Services. (2023). Health Industry Cybersecurity Practices (HICP).

[21] European Union Agency for Cybersecurity (ENISA). (2021). Threat Landscape for Healthcare.