© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723017

Cybersecurity Risk and Digital Resilience in Healthcare Information Systems: Strategies for Protecting Data Integrity and Patient Safety

DESIRE EMEKA[1], FIDELIA AHIANTE[2]
[1] *Southern Illinois University Edwardsville*
[2] *Prairie View A&M University Texas*

Abstract- ***The increasing reliance on digital technologies has transformed the delivery, management, and coordination of healthcare services. Electronic health records, connected medical devices, telehealth platforms, cloud computing, health information exchanges, and other digital systems have improved the availability and exchange of healthcare information while simultaneously increasing the number of systems and connections that must be protected against cybersecurity threats (Luna et al., 2016; World Health Organization [WHO], 2025). Cybersecurity incidents in healthcare can have consequences that extend beyond the loss of confidential information because disruption, unauthorized modification, or unavailability of health information may interfere with clinical workflows and patient care (Argaw et al., 2020; Kruse et al., 2017). This article examines the relationship between cybersecurity risk, data integrity, digital resilience, and patient safety in healthcare information systems. An integrative review of peer reviewed literature and authoritative cybersecurity guidance was used to identify recurring cybersecurity risks, organizational vulnerabilities, and resilience strategies. The literature indicates that ransomware, unauthorized access, vulnerabilities in connected medical devices, human factors, legacy systems, inadequate access controls, and weaknesses in third party environments remain important cybersecurity concerns in healthcare (Ewoh & Dua, 2024; Luna et al., 2016). Evidence also indicates that cyber incidents can disrupt emergency departments, increase patient volumes at neighboring facilities, delay clinical services, and create operational conditions that may affect patient safety (Choi et al., 2024; Neprash et al., 2024). Based on these findings, this article proposes a Digital Resilience and Patient Safety Framework that integrates risk identification, data integrity protection, preventive security, resilient response and recovery, and continuous organizational learning. The framework positions cybersecurity as an organizational and patient safety responsibility rather than solely an information technology function. The article concludes that healthcare organizations should evaluate cybersecurity controls according to their ability not only to protect information from unauthorized access but also to preserve the accuracy, availability, reliability, and continuity of information required for safe healthcare delivery.***

Keywords: healthcare cybersecurity, digital resilience, healthcare information systems, data integrity, patient safety, electronic health records, ransomware, information security

I. INTRODUCTION

Digital technologies have become deeply integrated into contemporary healthcare delivery. Electronic health records allow healthcare professionals to document and retrieve clinical information, while connected medical devices, telehealth platforms, cloud services, and health information exchange systems support communication and information sharing across healthcare environments (Kierkegaard, 2011; Rezaeibagha et al., 2015). The expansion of these technologies has increased the volume and interconnectedness of healthcare information systems, creating additional dependencies that must be managed to maintain security and reliable healthcare operations (Ewoh & Dua, 2024; WHO, 2025).

Healthcare information systems contain information that is valuable to patients, healthcare providers, insurers, researchers, and malicious actors. Health records can contain clinical histories, medication information, diagnostic results, insurance information, demographic information, and other sensitive information, making healthcare organizations attractive targets for cybercrime (Luna et al., 2016; Kruse et al., 2017). Systematic reviews have identified unauthorized access, malware, ransomware, social engineering, denial of service, insider threats, and vulnerabilities in connected systems among the

cybersecurity threats affecting healthcare environments (Luna et al., 2016; Aljuraid & Justinia, 2022).

The consequences of cybersecurity incidents can extend beyond confidentiality and privacy. Healthcare organizations depend on information systems to support clinical decision making, communication, medication management, diagnostic services, scheduling, billing, and other activities required for healthcare delivery (Argaw et al., 2020; Ewoh & Dua, 2024). Consequently, a system that becomes unavailable or produces unreliable information can create operational and clinical challenges even when no patient record is permanently lost (Ewoh & Dua, 2024; Kruse et al., 2026).

Ransomware provides a particularly clear example of this relationship between cybersecurity and patient safety. A study of ransomware attacks affecting United States healthcare delivery organizations between 2016 and 2021 identified 374 attacks and reported that the annual number of attacks more than doubled during the study period (Neprash et al., 2024). The same research found that the attacks exposed information belonging to nearly 42 million individuals and increasingly affected larger organizations with multiple facilities (Neprash et al., 2024).

The operational consequences of ransomware can also extend beyond the organization directly targeted. Choi et al. (2024) examined emergency departments located near healthcare facilities affected by a ransomware attack and found increases in emergency department census, ambulance arrivals, waiting times, patients leaving without being seen, length of stay, and emergency medical services diversion during the attack and recovery period.

These findings demonstrate why cybersecurity in healthcare should not be treated exclusively as a technical issue. A healthcare organization may have strong privacy controls but still be vulnerable if it cannot maintain access to essential information during a cyber incident. Similarly, an organization may restore a system after an incident but still face patient safety risks if the integrity of restored information has not been established.

The U.S. Department of Health and Human Services has increasingly emphasized this relationship by describing cyber safety as a component of patient safety and developing voluntary Healthcare and Public Health Cybersecurity Performance Goals intended to improve cyber preparedness, resilience, and protection of patient information and safety (U.S. Department of Health and Human Services [HHS], 2024).

The purpose of this article is therefore to examine cybersecurity risk and digital resilience in healthcare information systems, with particular attention to the protection of data integrity and patient safety. The article synthesizes existing research and develops a practical framework for connecting cybersecurity management with healthcare continuity and patient safety.

II. PROBLEM STATEMENT

Healthcare organizations face a cybersecurity environment characterized by increasing technological interconnection, dependence on digital information, and exposure to diverse cyber threats (Ewoh & Dua, 2024; WHO, 2025). A systematic review of healthcare cybersecurity literature identified technological, organizational, human, and process related factors as contributors to cybersecurity vulnerability, demonstrating that healthcare security cannot be addressed through technical controls alone (Ewoh & Dua, 2024).

The problem is further complicated by the clinical importance of healthcare information. Electronic health records are not simply repositories of personal information. They contain information that healthcare professionals use to assess patients, coordinate treatment, document clinical decisions, and support continuity of care (Fernández Alemán et al., 2013; Rezaeibagha et al., 2015). Therefore, unauthorized modification or unavailability of information can create risks that are different from those associated with ordinary business information systems.

Research on electronic health record security has identified access control, authentication, audit logging, encryption, interoperability, consent mechanisms, and security policies as important components of secure healthcare information systems

(Fernández Alemán et al., 2013; Rezaeibagha et al., 2015). However, security controls are often discussed in relation to confidentiality and privacy rather than their relationship with clinical continuity and patient safety.

This creates a research and practice gap. Healthcare organizations need cybersecurity programs that address confidentiality while simultaneously protecting the integrity and availability of information required for safe healthcare delivery. Digital resilience provides a useful perspective because it focuses not only on preventing cyber incidents but also on preparing for disruption, responding effectively, recovering essential services, and learning from cybersecurity events (National Institute of Standards and Technology [NIST], 2024).

III. RESEARCH OBJECTIVES

The primary objective of this research is to examine how cybersecurity risk management and digital resilience can be integrated to protect healthcare information systems and support patient safety.

The specific objectives are to:

Identify major cybersecurity risks affecting healthcare information systems.
Examine how cybersecurity incidents can affect healthcare operations and patient safety.
Examine the importance of data integrity in electronic healthcare environments.
Identify technological, human, and organizational factors that influence healthcare cybersecurity resilience.
Develop a conceptual framework that connects cybersecurity risk management with digital resilience and patient safety.
Recommend strategies that healthcare organizations can use to strengthen information security and continuity of care.

IV. RESEARCH QUESTIONS

This article addresses five research questions:

RQ1: What cybersecurity risks pose significant threats to the integrity and availability of healthcare information systems?

RQ2: How can cybersecurity incidents affect healthcare operations and patient safety?

RQ3: What technological, human, and organizational factors influence digital resilience in healthcare?

RQ4: What cybersecurity strategies can healthcare organizations use to protect healthcare data integrity?

RQ5: How can cybersecurity governance be integrated into broader healthcare risk management and patient safety practices?

V. METHODOLOGY

Research Design

This study uses an integrative literature review and conceptual synthesis. An integrative approach is appropriate for examining healthcare cybersecurity because the subject incorporates findings from information systems, cybersecurity, healthcare management, clinical safety, medical device security, and organizational risk management (Ewoh & Dua, 2024; Kruse et al., 2026).

The literature considered in this study includes peer reviewed journal articles, systematic reviews, government publications, cybersecurity frameworks, and international health guidance. Peer reviewed sources were prioritized for empirical and research based claims, while authoritative government and international sources were used to establish cybersecurity recommendations, standards, and policy guidance.

The literature was organized around five themes: cybersecurity threats, data integrity, patient safety, digital resilience, and organizational governance. These themes were then synthesized to develop the

Digital Resilience and Patient Safety Framework proposed in this article.

Source Selection

The literature included studies examining healthcare cybersecurity, electronic health record security, ransomware, medical device security, access control, privacy, patient safety, digital health, and organizational resilience. Systematic reviews were given particular attention because they synthesize evidence from multiple studies and provide broader perspectives on cybersecurity risks and controls (Fernández Alemán et al., 2013; Ewoh & Dua, 2024; Kruse et al., 2026).

NIST Cybersecurity Framework 2.0 was used as a major reference for cybersecurity risk management because it provides a flexible structure for organizations to understand, assess, prioritize, and communicate cybersecurity risk (NIST, 2024). HHS Healthcare and Public Health Cybersecurity Performance Goals were used to incorporate healthcare specific cybersecurity recommendations related to vulnerability management, endpoint protection, access control, incident preparedness, and resilience (HHS, 2024). WHO guidance was used to incorporate broader digital health cybersecurity and privacy considerations (WHO, 2025).

VI. CYBERSECURITY RISKS IN HEALTHCARE INFORMATION SYSTEMS

6.1 Unauthorized Access

Unauthorized access remains an important concern in healthcare information systems because electronic health records contain sensitive clinical and personal information (Fernández Alemán et al., 2013; Luna et al., 2016). Systematic research on electronic health record security has identified authentication, access control, authorization, audit logging, and encryption among the major technical mechanisms used to protect health information (Fernández Alemán et al., 2013; Rezaeibagha et al., 2015).

Access control is particularly important because healthcare workers require different levels of access depending on their responsibilities. A clinician may require access to clinical information that is unnecessary for an administrative employee, while an information technology administrator may require technical access without needing unrestricted access to clinical records (Kierkegaard, 2011; Rezaeibagha et al., 2015). Research on electronic health record access control has therefore examined role based, contextual, temporal, and risk based approaches for controlling access to health information (Abouelmehdi et al., 2017).

Healthcare organizations should consequently implement access controls that follow the principle of granting users only the access necessary for their responsibilities while maintaining appropriate mechanisms for emergency access (Fernández Alemán et al., 2013; Abouelmehdi et al., 2017). Audit trails are also important because they provide records of system activity that can support monitoring, investigation, and accountability (Fernández Alemán et al., 2013).

6.2 Ransomware

Ransomware is one of the most significant cybersecurity threats affecting healthcare organizations because attacks can disrupt access to information systems and interfere with healthcare operations (Neprash et al., 2024; Kruse et al., 2017).

Neprash et al. (2024) analyzed 374 ransomware attacks against healthcare delivery organizations in the United States between 2016 and 2021 and found that the number of attacks more than doubled during the study period. The attacks exposed information associated with nearly 42 million individuals, demonstrating the potential scale of healthcare ransomware incidents (Neprash et al., 2024).

The consequences of ransomware can extend beyond the organization experiencing the attack. Choi et al. (2024) found that a ransomware attack affecting one healthcare organization was associated with increased patient volumes, ambulance arrivals, waiting times, and emergency medical services diversion at nearby emergency departments.

These findings suggest that healthcare ransomware should be considered a continuity of care and patient

safety issue rather than only a data security issue. HHS similarly identifies cyber resilience and patient safety as related objectives in its healthcare specific Cybersecurity Performance Goals (HHS, 2024).

6.3 Medical Device Vulnerabilities

Modern healthcare environments increasingly rely on medical devices that connect to hospital networks, other medical devices, and external systems (U.S. Food and Drug Administration [FDA], 2025). The connectivity that allows devices to exchange information and support healthcare services can also increase cybersecurity exposure (FDA, 2025).

The FDA recognizes that cybersecurity vulnerabilities can affect the safety and effectiveness of connected medical devices and emphasizes cooperation among manufacturers, healthcare organizations, and other stakeholders to manage cybersecurity risks (FDA, 2025).

The regulatory environment has also evolved in the United States. Section 524B of the Federal Food, Drug, and Cosmetic Act established cybersecurity requirements for certain medical devices submitted to the FDA after March 29, 2023, including requirements related to cybersecurity processes and software components (FDA, 2025).

Medical device cybersecurity therefore needs to be integrated into broader healthcare cybersecurity programs rather than treated as a separate technical responsibility.

6.4 Legacy Technology

Legacy technologies can create cybersecurity challenges because older systems may be difficult to patch, replace, or integrate with modern security tools (Ewoh & Dua, 2024). The healthcare sector can be particularly affected because organizations may depend on specialized systems and medical technologies that have long operational lifecycles (Ewoh & Dua, 2024; FDA, 2025).

The presence of legacy technology does not automatically mean that a system is insecure. However, unsupported software, unavailable security updates, inadequate monitoring, and poorly documented dependencies can increase organizational risk (HHS, 2024; NIST, 2024).

Healthcare organizations should therefore maintain inventories of their information assets and identify systems that require additional compensating controls because they cannot be easily upgraded or replaced (HHS, 2024).

6.5 Human Factors

Cybersecurity in healthcare is influenced by human behavior as well as technology. A systematic review of healthcare cybersecurity found that vulnerabilities arise through interactions among technology, people, processes, and organizational conditions (Ewoh & Dua, 2024).

Security controls that are poorly aligned with clinical workflows can create practical difficulties for healthcare workers. The literature therefore supports sociotechnical approaches that consider human behavior, organizational processes, training, technology design, and clinical requirements together (Ewoh & Dua, 2024).

Healthcare cybersecurity education should consequently extend beyond basic compliance training. Organizations should help employees understand how phishing, credential compromise, inappropriate access, and other behaviors can contribute to cybersecurity incidents (Ewoh & Dua, 2024).

VII. DATA INTEGRITY IN HEALTHCARE INFORMATION SYSTEMS

Data integrity refers to the preservation of information accuracy, consistency, completeness, and reliability throughout its lifecycle. In healthcare environments, data integrity is especially important because clinicians depend on electronic information to support assessment, diagnosis, treatment, and coordination of care (Fernández Alemán et al., 2013; Rezaeibagha et al., 2015).

A confidentiality breach exposes information to unauthorized parties, whereas an integrity failure can

cause authorized users to rely on inaccurate information. This distinction makes data integrity a particularly important cybersecurity concern in clinical environments (Argaw et al., 2020).

Access control can contribute to data integrity by restricting who is authorized to create, modify, or delete information (Abouelmehdi et al., 2017). Audit logging can provide evidence of changes and system activity, while authentication mechanisms help establish whether system activity can be associated with authorized users (Fernández Alemán et al., 2013).

Encryption can protect information while it is being stored or transmitted, although encryption alone does not guarantee that information remains accurate or that an authorized user cannot intentionally modify it (Rezaeibagha et al., 2015). Effective data integrity protection therefore requires multiple complementary controls rather than dependence on a single technology.

Backup systems also play an important role in integrity and recovery. A backup that cannot be restored reliably cannot provide meaningful protection during a major incident. Consequently, organizations should periodically test restoration procedures and verify that recovered systems and information are usable before an incident occurs (NIST, 2024; HHS, 2024).

VIII. CYBERSECURITY AND PATIENT SAFETY

The relationship between cybersecurity and patient safety becomes most visible when information systems are disrupted.

Healthcare professionals often depend on electronic systems to retrieve patient information, document care, communicate with other professionals, access laboratory results, review medications, and perform other clinical activities (Fernández Alemán et al., 2013). When these systems become unavailable, organizations may need to use alternative processes that can increase operational complexity (Ewoh & Dua, 2024).

Empirical evidence demonstrates that cyber incidents can have effects beyond the organization that is directly attacked. Choi et al. (2024) found that ransomware affecting hospitals was associated with increased demand and operational pressure at nearby emergency departments.

Research examining ransomware attacks against healthcare organizations has similarly concluded that disruptions associated with cyberattacks may threaten patient safety and healthcare outcomes (Neprash et al., 2024).

Cybersecurity should therefore be incorporated into patient safety planning. HHS explicitly identifies cyber safety as patient safety and has developed healthcare cybersecurity goals intended to strengthen preparedness, resilience, and protection of patient health information and safety (HHS, 2024).

IX. DIGITAL RESILIENCE IN HEALTHCARE

Digital resilience refers to an organization's capacity to prepare for disruption, withstand adverse events, respond effectively, recover important functions, and adapt based on lessons learned (NIST, 2024). NIST Cybersecurity Framework 2.0 provides a structured approach for organizations to understand, assess, prioritize, and communicate cybersecurity risk (NIST, 2024).

For healthcare organizations, resilience must account for the clinical consequences of technology disruption. The most important question is not simply whether an information system can be restored but whether critical healthcare services can continue safely while restoration is occurring.

WHO guidance on cybersecurity and privacy maturity assessment similarly emphasizes that digital health organizations should assess security and privacy across governance, data management, transmission security, monitoring, and user behavior (WHO, 2025).

A resilient healthcare organization should therefore understand its critical digital dependencies and establish procedures for maintaining essential operations during system disruptions.

X. PROPOSED DIGITAL RESILIENCE AND PATIENT SAFETY FRAMEWORK

Based on the literature reviewed in this article, a five component Digital Resilience and Patient Safety Framework is proposed.

10.1 Component One: Risk Identification

The first component is continuous identification and assessment of cybersecurity risks.

Healthcare organizations should maintain inventories of critical information systems, connected devices, applications, data repositories, cloud services, and external connections (HHS, 2024; NIST, 2024).

Risk assessments should also consider clinical consequences. A system supporting intensive care, medication administration, emergency services, laboratory testing, or diagnostic imaging may require different resilience priorities from a system supporting nonclinical administrative functions.

10.2 Component Two: Data Integrity Protection

The second component focuses on maintaining trustworthy healthcare information.

Organizations should implement authentication, access control, audit logging, encryption, change monitoring, and backup controls to protect health information throughout its lifecycle (Fernández Alemán et al., 2013; Rezaeibagha et al., 2015).

Data integrity protection should also include procedures for validating restored information after a cybersecurity incident. Restoring access to a system without verifying the accuracy and completeness of critical information may leave unresolved clinical risks.

10.3 Component Three: Preventive Security Controls

The third component involves layered preventive security.

NIST recommends a risk based approach to cybersecurity rather than reliance on a single security technology (NIST, 2024). HHS healthcare Cybersecurity Performance Goals similarly identify practices involving vulnerability management, endpoint protection, identity management, email security, and other controls intended to reduce common cybersecurity risks (HHS, 2024).

Healthcare organizations should therefore combine multiple security controls according to their risk profiles.

10.4 Component Four: Resilient Response and Recovery

The fourth component focuses on maintaining and restoring healthcare services during cybersecurity incidents.

Incident response plans should identify critical services, responsibilities, communication procedures, downtime processes, backup restoration procedures, and recovery priorities (HHS, 2024; NIST, 2024).

Healthcare organizations should also conduct exercises that involve clinical personnel because cybersecurity incidents can affect clinical workflows rather than information technology systems alone (FDA, 2025; HHS, 2024).

10.5 Component Five: Continuous Organizational Learning

The fifth component involves learning from cybersecurity events and exercises.

NIST's risk management approach emphasizes continuous assessment and improvement of cybersecurity activities (NIST, 2024). WHO's cybersecurity maturity assessment guidance likewise encourages organizations to evaluate their security posture and identify areas for improvement (WHO, 2025).

Healthcare organizations should therefore examine incidents and exercises to determine what occurred, which controls were effective, which controls failed, which clinical services were affected, and what changes should be implemented.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723017

XI. DISCUSSION

The literature reviewed in this article demonstrates that healthcare cybersecurity is a multidimensional problem involving technology, people, organizational processes, and clinical operations (Ewoh & Dua, 2024).

Traditional information security models emphasize confidentiality, integrity, and availability. These principles remain important for healthcare systems because patient information must be protected from unauthorized disclosure, unauthorized modification, and inappropriate loss of access (Fernández Alemán et al., 2013; Rezaeibagha et al., 2015).

However, healthcare introduces an additional consideration because information systems directly support clinical activities. A cybersecurity incident can therefore become an operational and patient safety event when it prevents healthcare professionals from accessing information or using systems required for patient care (Argaw et al., 2020; Choi et al., 2024).

The proposed framework responds to this problem by integrating cybersecurity controls with resilience and patient safety. The framework does not suggest that every healthcare organization should implement identical technologies. Instead, it emphasizes risk based prioritization.

This approach is consistent with NIST Cybersecurity Framework 2.0, which allows organizations to select cybersecurity outcomes according to their specific circumstances rather than prescribing a single technical implementation (NIST, 2024).

The framework also aligns with HHS healthcare cybersecurity guidance, which identifies high impact cybersecurity practices that healthcare organizations can prioritize to improve cyber preparedness and resilience (HHS, 2024).

Another important finding is the need to integrate medical device security into organizational cybersecurity. The FDA recognizes that connected medical devices can create cybersecurity risks that may affect device safety and effectiveness (FDA, 2025). This means that cybersecurity planning should include clinical engineering, biomedical engineering, information technology, cybersecurity, risk management, and clinical leadership.

The human dimension is equally important. The systematic review by Ewoh and Dua (2024) demonstrates that healthcare cybersecurity should be approached as a sociotechnical problem because technological vulnerabilities interact with people and organizational processes.

Consequently, cybersecurity programs should avoid placing responsibility entirely on individual employees. Organizations should design secure systems, provide appropriate training, simplify secure workflows, establish reasonable access procedures, and create an organizational culture in which cybersecurity is recognized as part of safe healthcare delivery.

XII. PRACTICAL RECOMMENDATIONS

12.1 Integrate Cybersecurity With Patient Safety Governance

Healthcare organizations should include cybersecurity within broader enterprise risk management and patient safety programs because cyber incidents can affect healthcare delivery and patient safety (HHS, 2024; Choi et al., 2024).

12.2 Maintain a Complete Technology Inventory

Organizations should maintain current inventories of information systems, connected devices, applications, and critical technology dependencies because asset visibility is necessary for effective cybersecurity risk management (HHS, 2024; NIST, 2024).

12.3 Strengthen Identity and Access Management

Healthcare organizations should use strong authentication, appropriate authorization, role based access, privileged account controls, and audit logging to reduce inappropriate access to health information (Fernández Alemán et al., 2013; Abouelmehdi et al., 2017).

12.4 Protect and Test Backups

Organizations should maintain protected backups and regularly test recovery procedures because the ability to restore essential systems is a central component of digital resilience (NIST, 2024; HHS, 2024).

12.5 Strengthen Medical Device Cybersecurity

Healthcare organizations should incorporate medical devices into cybersecurity inventories, vulnerability assessments, incident response planning, and recovery exercises because connected medical devices can introduce cybersecurity risks that may affect safety and effectiveness (FDA, 2025).

12.6 Improve Workforce Cybersecurity Education

Cybersecurity training should address realistic healthcare scenarios and explain the relationship between secure behavior and patient safety because cybersecurity vulnerabilities can arise through interactions among technology, people, and organizational processes (Ewoh & Dua, 2024).

12.7 Manage Third Party Cybersecurity Risk

Healthcare organizations should assess cybersecurity risks associated with vendors, cloud providers, software suppliers, and other external partners because healthcare information systems increasingly depend on interconnected external services (WHO, 2025; HHS, 2024).

12.8 Conduct Regular Cybersecurity Exercises

Organizations should conduct exercises involving ransomware, system outages, medical device disruption, loss of electronic health records, and communication failures because cyber incidents can affect clinical operations and surrounding healthcare organizations (Choi et al., 2024; Tully et al., 2025).

12.9 Establish Resilience Metrics

Healthcare organizations should measure cybersecurity performance using indicators such as vulnerability remediation, critical asset coverage, incident detection, containment, recovery time, backup restoration success, and duration of clinical system downtime (NIST, 2024; HHS, 2024).

XIII. LIMITATIONS

This article has several limitations. First, the research is based on an integrative analysis of published literature and authoritative guidance rather than primary data collected directly from healthcare organizations. Second, cybersecurity threats and technologies evolve rapidly, meaning that emerging vulnerabilities and attack methods may not be represented in older studies. Third, healthcare organizations differ in size, technological maturity, financial resources, clinical services, and regulatory environments, which means that the proposed framework should be adapted to organizational circumstances rather than applied as a universal implementation model.

Future research should empirically evaluate the proposed framework in healthcare organizations of different sizes and types. Future studies could examine whether organizations with stronger cybersecurity maturity experience shorter periods of clinical disruption after cybersecurity incidents. Research could also examine relationships between cybersecurity maturity indicators and patient safety outcomes using longitudinal organizational data.

XIV. CONCLUSION

The increasing dependence of healthcare organizations on digital information systems has made cybersecurity an important component of healthcare risk management and patient safety (Ewoh & Dua, 2024; HHS, 2024).

Cybersecurity incidents can compromise confidentiality, but they can also affect the integrity and availability of information required for healthcare delivery (Fernández Alemán et al., 2013; Rezaeibagha et al., 2015). Research involving ransomware incidents demonstrates that cyberattacks can disrupt healthcare organizations and create operational effects that extend to nearby healthcare facilities (Choi et al., 2024; Neprash et al., 2024).

The evidence therefore supports a broader understanding of healthcare cybersecurity in which data protection, operational continuity, digital resilience, and patient safety are treated as interconnected objectives.

The Digital Resilience and Patient Safety Framework proposed in this article integrates five areas: risk identification, data integrity protection, preventive cybersecurity controls, resilient response and recovery, and continuous organizational learning. The framework builds on established cybersecurity principles while emphasizing the distinctive consequences of cybersecurity failure within healthcare environments (NIST, 2024; HHS, 2024; WHO, 2025).

The central conclusion is that healthcare cybersecurity should not be measured solely by the organization's ability to prevent unauthorized access or data breaches. A resilient healthcare organization must also be able to preserve trustworthy information, maintain essential services during disruption, recover systems safely, and learn from cybersecurity events.

As healthcare organizations continue to expand their use of connected technologies, cybersecurity will increasingly influence the reliability and continuity of healthcare delivery. Strengthening digital resilience is therefore not simply a technical investment. It is an organizational responsibility that contributes to the protection of healthcare information and the delivery of safe patient care.

REFERENCES

[1] Abouelmehdi, K., Beni Hassan, S., Khaloufi, H., & Azzouazi, M. (2017). Access control and privilege management in electronic health records: A systematic literature review. *Journal of Medical Systems, 41*, Article 123.

[2] Aljuraid, R., & Justinia, T. (2022). Classification of challenges and threats in healthcare cybersecurity: A systematic review. *Studies in Health Technology and Informatics, 295*, 362–365. Crossref

[3] Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*, 146. Crossref

[4] Choi, Y. J., Johnson, D., Koo, D. C., & colleagues. (2024). Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA Network Open, 7*(5), e2410824.

[5] Ewoh, P., & Dua, U. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. *Journal of Medical Internet Research, 26*, e46904.

[6] Fernández Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*(3), 541–562. Crossref

[7] Kierkegaard, P. (2011). Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review, 27*(5), 503–515. Crossref

[8] 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. Crossref

[9] Kruse, C. S., Dolezel, D., & Shanmugam, R. (2026). Cybersecurity in healthcare: A systematic review and narrative analysis. *Applied Clinical Informatics, 17*(2), 315–328. Crossref

[10] Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care, 24*(1), 1–9. Crossref

[11] National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce. Crossref

[12] Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., & Bohman, H. R. (2024). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum, 5*(1), e234782. Crossref

[13] Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Information Management Journal, 44*(3), 23–38. Crossref

[14] Tully, J. L., et al. (2025). Patient care technology disruptions associated with the CrowdStrike outage. *JAMA Network Open, 8*(7), e2530226. Crossref

[15] U.S. Department of Health and Human Services. (2024). *Healthcare and public health sector specific cybersecurity performance goals*. https://hhscyber.hhs.gov/cybersecurity-performance-goals.html

[16] U.S. Food and Drug Administration. (2025). *Cybersecurity in medical devices*. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

[17] World Health Organization. (2025). *Cybersecurity and privacy maturity assessment and strengthening for digital health information systems*. WHO Regional Office for Europe. https://www.who.int/europe/publications/i/item/WHO-EURO-2025-11827-51599-78854