International Journal of Multidisciplinary Innovation and Research Methodology (IJMIRM)
ISSN: 2960-2068, Volume 4, Issue 3, July-September, 2025, Available online at: https://ijmirm.com

# Cybersecurity Threat Intelligence Frameworks in Healthcare Data Systems

**Muath Rebdi AlRebdi[1], Sultan Khalid AlQahtani[2]**

[1,] Health Information Systems, Alnakheel Medical Complex ,Riyadh, Saudi Arabia
[2,]Health Information System, King Fahad hospital,Riyadh, Saudi Arabia

## ABSTRACT

**Background:-**The digital transformation of healthcare, driven by electronic health records (EHRs), telemedicine, and the Internet of Medical Things (IoMT), has revolutionized patient care but simultaneously exposed healthcare systems to unprecedented cybersecurity threats. Ransomware, phishing, insider threats, and third-party risks now jeopardize patient safety, data privacy, and operational continuity, making cybersecurity a critical pillar of modern healthcare.

**Methodology:-**This review explores scientific and evidence-based approaches to cybersecurity in healthcare, focusing on the integration of threat intelligence into established frameworks such as NIST CSF, HIPAA Security Rule, ISO/IEC 27001, HITRUST CSF, and COBIT. The methodology draws upon published studies, regulatory standards, and applied threat intelligence models including threat modeling, risk assessment, AI-driven analytics, and continuous monitoring mechanisms.

**Results:-**Findings reveal that adopting robust cybersecurity frameworks enhanced by threat intelligence significantly improves the healthcare sector's ability to detect, prevent, and respond to cyberattacks. Simulation models, machine learning–based detection, and collaborative intelligence platforms (e.g., Health-ISAC) enhance situational awareness, reduce response times, and build resilience. However, challenges persist, including limited resources, legacy infrastructures, interoperability gaps, ethical concerns around data sharing, and the digital divide across healthcare organizations.

**Conclusion:-**Cybersecurity threat intelligence frameworks provide a structured, proactive defense strategy essential for safeguarding sensitive health data and ensuring patient safety. While barriers remain, the integration of AI-driven detection, automation, and collaborative intelligence sharing offers promising opportunities to enhance resilience. Moving forward, balancing technological innovation with regulatory compliance, ethical standards, and equitable resource allocation will be critical to building a secure and adaptive healthcare cybersecurity culture.

**Keywords: Cybersecurity, Healthcare data systems, Threat intelligence, NIST CSF, HIPAA, IoMT security, Artificial intelligence, Patient safety.**

## INTRODUCTION

### Rising Importance of Cybersecurity in Healthcare

The healthcare sector is undergoing a profound digital transformation that has broad implications for patient care, operational efficiency, and data management. With the advent of electronic health records (EHRs), telemedicine, mobile health apps, and the Internet of Medical Things (IoMT), healthcare has become deeply reliant on complex information technology (IT) systems.(1) While these advances have revolutionized medicine, they have also introduced critical cybersecurity challenges that directly impact patient safety, privacy, and the overall integrity of healthcare delivery. As healthcare data becomes more digitized and interconnected, safeguarding this data rises from mere regulatory compliance to a foundational pillar of trust between patients and providers. Cybersecurity is no longer only a technical issue but a core healthcare concern because breaches or disruptions can lead to incorrect diagnoses, ineffective treatments, delayed care, and even loss of life. Large-scale cyberattacks targeting hospitals have become alarmingly frequent, with ransomware attacks being among the most disruptive, shutting down systems and demanding extortion payments.(2) The fallout from such incidents extends beyond financial loss to include jeopardizing patient outcomes and eroding public confidence. This heightened threat landscape underscores the critical importance of establishing robust cybersecurity frameworks, specifically tailored to healthcare's unique environment. These frameworks are grounded in scientific methodologies and guide organizations through the identification, assessment, and mitigation of cyber risks.(3) They integrate technological defenses with policy, staff training, and incident response planning, fostering a holistic approach to cybersecurity.

Further complicating this landscape is the diverse range of healthcare data systems—each with different vulnerabilities and security requirements. The healthcare ecosystem includes not only hospitals and clinics but also research institutions, medical device manufacturers, software vendors, insurers, and third-party service providers, all

interconnected in a web of data exchange. This complexity requires that cybersecurity strategies be built on a deep understanding of data flows, threat actors, and potential attack vectors.

Moreover, the highly regulated nature of healthcare data, protected under laws such as HIPAA in the U.S. and GDPR in Europe, necessitates compliance with rigorous privacy and security standards.(4) The challenge lies in balancing stringent security measures with seamless accessibility required for timely clinical decision-making and patient care.
To meet these evolving challenges, cybersecurity in healthcare is increasingly adopting a science-based, methodological approach. This approach relies on evidence-based frameworks, threat intelligence, and continuous improvement practices. It draws from fields such as information science, behavioral science, and systems engineering to establish resilient healthcare infrastructures capable of adapting to emerging threats.

## 2. Healthcare Data Systems and Threat Landscape

Healthcare data systems are multifaceted, encompassing a range of technologies that collectively manage the collection, storage, analysis, and exchange of health-related information. The security of these systems is paramount given the sensitivity of healthcare data and the real-time implications of system availability.

### 2.1.Electronic Health Records (EHRs):

EHRs are digital versions of patients' paper charts and contain comprehensive health information including medical history, diagnoses, medications, immunization records, laboratory results, and imaging data. They enable care coordination across multiple providers and settings. However, the centralized storage of vast amounts of sensitive personal data makes EHR databases attractive targets for cybercriminals.(5) The healthcare sector has been repeatedly targeted by ransomware and data breaches exploiting vulnerabilities in EHR software or through phishing attacks aimed at healthcare staff.

### 2.2.Internet of Medical Things (IoMT):

IoMT refers to connected medical devices and sensors that collect and transmit health data for monitoring and treatment purposes. Examples include wearable devices, pacemakers, infusion pumps, and remote monitoring systems. These devices enhance healthcare but present unique security challenges because many operate with limited processing power and security features, often lacking the capacity to support complex encryption or authentication protocols. (6)Additionally, the integration of IoMT into hospital networks expands the attack surface, with vulnerabilities potentially allowing attackers to manipulate devices and compromise patient safety.

### 2.3.Healthcare Databases:

Beyond patient records, healthcare databases include research data, billing information, and administrative records. These repositories support analytics, clinical decision support systems, and operational management. They typically support various access privileges to accommodate research, clinical, and operational use, creating complexity in regulating access controls.(7) Insider threats, whether intentional data theft or accidental misuse by authorized users, represent significant risks in this context.

### 2.4.Key Cyber Threats:

**2.4.1.Ransomware:** Ransomware attacks have escalated as one of the most significant threats to healthcare worldwide. Attackers deploy malicious software to encrypt essential files and demand ransom payments to restore access. The disruption can cripple healthcare delivery since access to EHRs, imaging systems, and diagnostic labs is often essential for patient care. Hospitals impacted by ransomware often face prolonged downtime, risking patient safety and operational chaos.(8)

**2.4.2.Phishing Attacks:** Often regarded as the starting point for many cyber intrusions, phishing attacks exploit human vulnerabilities in healthcare organizations. Attackers send deceptive emails that trick recipients into divulging login credentials or deploying malware. Given the high pressure and fast pace in healthcare settings, staff members may inadvertently click malicious links or attachments, enabling attackers to gain footholds in critical systems.(9)

**2.4.3.Insider Threats:** Insiders include employees, contractors, or partners with legitimate access who either intentionally or negligently compromise security. These threats are difficult to detect as insiders can bypass technological defenses using valid credentials. Motivations vary from financial gain to disgruntlement, or accidental exposure due to insufficient training or awareness.(10) The insider threat also includes errors, such as misconfigurations or sharing of sensitive data without proper authorization.

**2.4.4.Third-Party Risks:** Healthcare systems depend heavily on vendors and third-party service providers for software, cloud hosting, and specialized services. These third parties can introduce vulnerabilities if their own security is inadequate. Supply chain attacks, where attackers compromise smaller vendors to access larger healthcare targets, have become an increasing concern. Ensuring third-party cybersecurity compliance and continuous monitoring is critical yet challenging.(11)

**2.4.5.Impact and Challenges:**
The consequences of cyber threats in healthcare extend beyond data loss or theft. Compromised systems can lead to delays in treatment, misdiagnoses due to missing or altered data, and in worst cases, direct harm to patients if medical devices are manipulated. Furthermore, breaches can erode public trust, impacting patient willingness to disclose information and comply with treatment. Addressing these threats requires multilayered defenses including technical controls such as encryption, firewalls, and intrusion detection; organizational policies; staff training; and incident response readiness.(12) Healthcare organizations must maintain a dynamic security posture to keep pace with the ever-evolving threat landscape.

## 3. Theoretical Foundations of Threat Intelligence
Threat intelligence is an essential component of modern cybersecurity strategies, particularly in the healthcare domain where the stakes are extraordinarily high. It involves the systematic collection, analysis, and dissemination of information about existing or emerging threats to predict and prevent cyberattacks.

### 3.1.Definition and Relevance:
Threat intelligence can be understood as actionable knowledge about threat actors, their motives, capabilities, and tactics, as well as indicators of compromise (IOCs) and vulnerabilities they exploit. This intelligence enables organizations to move from reactive defense to proactive cybersecurity, improving situational awareness and decision-making under uncertainty. In healthcare, threat intelligence plays a vital role given the complex and rapidly changing cyber threat environment. (13)By understanding adversaries' behaviors and tools, healthcare defenders can better prioritize their efforts, tailor defenses, and design incident response plans that mitigate the most impactful risks.

### 3.2.Scientific Principles Underlying Frameworks:
**3.2.1.Threat Modeling:**
Threat modeling is a formal process that identifies assets, potential threats, system weaknesses, and the possible attack paths. It develops a structured understanding of how an adversary might exploit vulnerabilities. Common models include STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) and ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), which offer taxonomies for categorizing threats. In healthcare, threat modeling enables tailoring security measures to protect critical assets like patient data, medical devices, and system availability.(14)

**3.2.2.Risk Assessment:**
Risk assessment quantifies the likelihood and impact of threats exploiting vulnerabilities. It involves evaluating the severity of consequences, such as harm to patients or financial losses, and considers existing controls to determine residual risks. Risk management frameworks such as NIST's Risk Management Framework or ISO 27001 protocols incorporate these principles. Healthcare organizations use risk assessment to prioritize limited resources, ensuring that the most critical threats receive attention.(14)

**3.2.3.Data-Driven Intelligence and Automation:**
Modern threat intelligence frameworks leverage data science, machine learning, and advanced analytics to collect and analyze large volumes of security data from internal systems and external sources. Techniques such as graph neural networks have been employed to detect relationships among threat entities and predict attack patterns, thereby enhancing anticipatory capabilities.(15) Automated frameworks can rapidly ingest threat feeds, correlate data, and generate alerts, facilitating real-time defense.

**3.2.4.Continuous Monitoring and Feedback Loops:**
Effective threat intelligence frameworks incorporate continuous monitoring, regularly updating intelligence to reflect new vulnerabilities, malware signatures, and adversary behaviors. Feedback loops enable security teams to learn from incidents, adjust threat models, and improve predictive accuracy. (16)This adaptive mechanism is crucial in healthcare, where emerging technologies and threats evolve at a rapid pace.

**3.2.4.Integration into Healthcare Cybersecurity:**
The application of threat intelligence frameworks in healthcare involves interweaving these scientific concepts into institutional policies, technical architectures, and operational workflows. For instance, intelligence gathered might inform secure coding practices for medical software, targeted training programs for healthcare staff on specific phishing tactics, or configuration of network segmentation to contain ransomware spread.(17) Furthermore, the collaboration among different stakeholders clinicians, IT personnel, administrators, and third-party partners is essential to effectively translate threat intelligence into actionable defense measures. This multidisciplinary approach ensures a comprehensive security posture that aligns with healthcare's core mission: patient safety and care quality.

## 4. Overview of Key Cybersecurity Frameworks in Healthcare
In the rapidly evolving healthcare cybersecurity landscape, several well-established frameworks provide structured guidance to protect sensitive health data and IT infrastructure. These frameworks vary in focus, regulatory scope, and

applicability, but all aim to address the multifaceted cybersecurity needs of healthcare systems. They incorporate essential security controls, risk management practices, and compliance requirements tailored to the healthcare context. A comparative overview of key frameworks **(Table 1)** highlights their distinct areas of emphasis and regulatory alignment:

**Table 1: Distinct areas of emphasis and regulatory alignment:**

| Framework | Description | Key Areas Addressed | Regulatory Scope | Ref |
|---|---|---|---|---|
| **NIST Cybersecurity Framework (CSF)** | Developed by the U.S. National Institute of Standards and Technology, it provides a flexible, risk-based approach to managing cybersecurity threats. | Identify, Protect, Detect, Respond, Recover; Risk management; Incident response; Continuous monitoring | U.S. federal agencies; widely adopted in healthcare globally | (18) |
| **HIPAA Security Rule** | U.S. regulation focused on protecting electronic protected health information (ePHI) in healthcare. | Administrative, physical, and technical safeguards; Access control; Audit controls; Data integrity | U.S. healthcare providers, health plans, clearinghouses | (19) |
| **ISO/IEC 27001** | International standard for information security management systems (ISMS), applicable across sectors including healthcare. | Risk assessment; Security controls; Leadership and policy; Continuous improvement | Global applicability across industries including healthcare | (20) |
| **HITRUST CSF** | Healthcare-specific framework combining federal and state regulations and industry best practices. | Data protection; Risk management; HIPAA compliance; Privacy; Security training | U.S. healthcare and related organizations | (21) |
| **COBIT (Control Objectives for Information and Related Technologies)** | IT governance framework offering comprehensive controls and metrics, useful for healthcare IT management. | IT governance; Risk management; Performance measurement; Security controls | Broad applicability, including healthcare | (22) |

The **NIST CSF** is one of the most widely implemented frameworks in healthcare, recognized for its comprehensive approach and ability to scale to organizations' size and risk profiles. NIST CSF's five core functions (Identify, Protect, Detect, Respond, Recover) guide healthcare institutions through the lifecycle of cybersecurity risk management, integrating technical, organizational, and procedural controls(18). The framework supports alignment with HIPAA requirements and other regulations while facilitating continuous improvement through risk assessments and security metrics.

**HIPAA Security Rule** remains fundamental in the U.S. healthcare sector, establishing mandatory standards for safeguarding ePHI. HIPAA requires covered entities to implement measures such as access controls, encryption, audit trails, and workforce training. While HIPAA sets the baseline for compliance, it is often supplemented by other frameworks for broader cybersecurity governance.(19)

**4.1.ISO/IEC 27001** offers an internationally recognized approach to establishing an information security management system (ISMS), aligning well with healthcare's need for formalized risk management and continual monitoring. Healthcare organizations adopting ISO standards benefit from rigorous documentation, leadership accountability, and systematic control implementation.(20)

**4.2.HITRUST CSF** specifically addresses the healthcare environment by harmonizing HIPAA requirements with other federal and state regulations and industry best practices. Healthcare providers and payers often use HITRUST certification to demonstrate a mature cybersecurity posture to partners and regulators.(21)

**4.3.COBIT**, while more general, provides healthcare IT managers with robust governance and risk management controls, focusing on the alignment of IT with business goals and effective performance metrics.(22)
Each framework's applicability depends on the healthcare organization's size, jurisdiction, and specific regulatory obligations. Often, healthcare entities integrate multiple frameworks to ensure comprehensive protection, regulatory compliance, and adaptive risk management.

**5. Threat Intelligence Integration for Healthcare**
Integrating threat intelligence into healthcare cybersecurity frameworks enhances organizations' ability to anticipate and neutralize cyber threats proactively. Threat intelligence involves collecting, analyzing, and sharing data about ongoing and emerging cyber threats and vulnerabilities. The integration process transforms raw threat data into actionable knowledge, enabling informed decision-making and timely defensive actions. The frameworks incorporate threat intelligence across several technical and procedural domains **(Figure 1).**

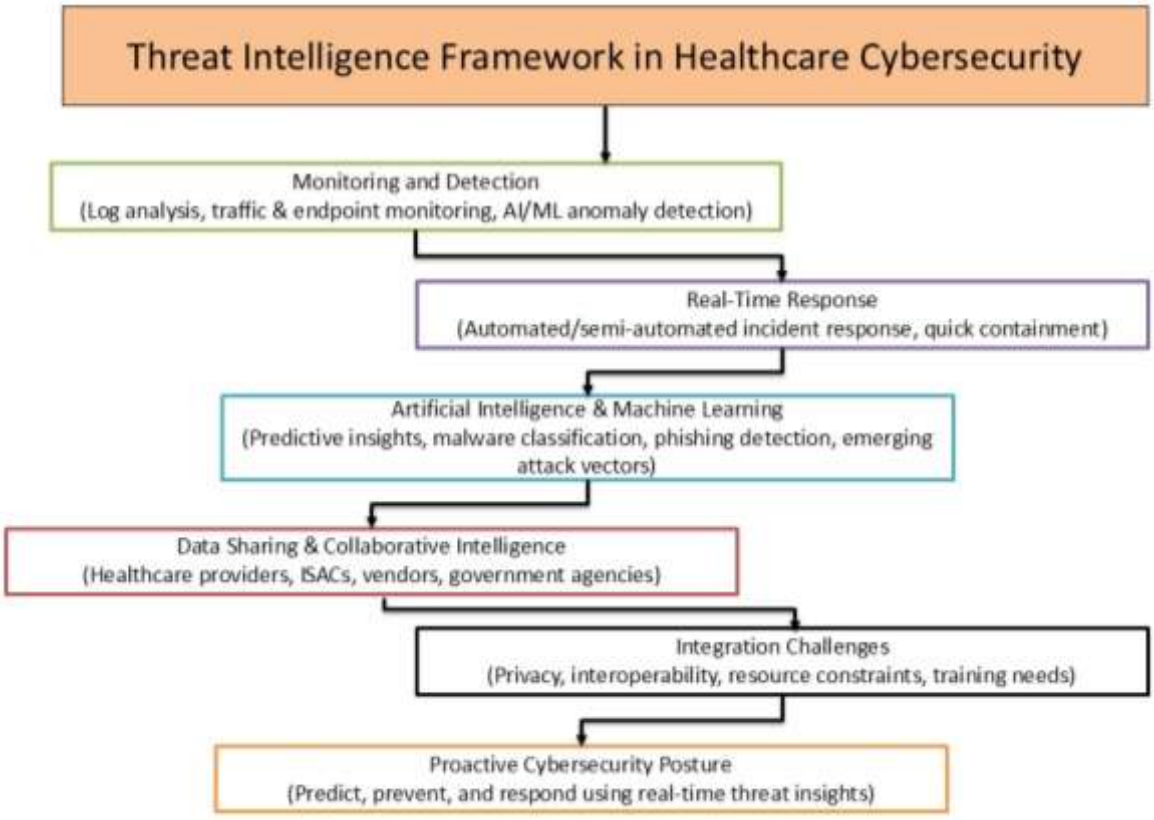


**Figure 1: Threat intelligence across several technical**

**5.1.Monitoring and Detection:** Healthcare environments leverage continuous monitoring tools to detect anomalies and indicators of compromise (IOCs). Through log analysis, network traffic examination, and endpoint monitoring, integrated threat intelligence feeds alert security teams to potential intrusions. Advanced detection systems, often enhanced by artificial intelligence (AI) and machine learning, identify subtle threat patterns that traditional signature-based systems might miss.(23) Anomaly detection algorithms can spot unusual access to EHR systems or abnormal communication between medical devices.

**5.2.Real-Time Response:** Effective frameworks promote automated or semi-automated incident response capabilities that utilize threat intelligence to prioritize alerts and orchestrate mitigation activities. Real-time response reduces dwell time of adversaries, limiting damage.(24) In healthcare, where downtime can risk patient lives, quick containment supported by threat intelligence is vital.

**5.2.Artificial Intelligence and Machine Learning:** These technologies play a crucial role in processing vast amounts of threat data and deriving predictive insights. AI models can classify malware, detect phishing campaigns, and forecast emerging attack vectors by learning from historical incidents. For healthcare specifically, AI-driven analytics help correlate device logs, patient data access patterns, and external threat feeds to identify sophisticated targeted attacks.(25)

**5.4.Data Sharing and Collaborative Intelligence:**
Cybersecurity frameworks increasingly emphasize sharing threat intelligence among healthcare providers, government agencies, and third-party vendors. This collaborative intelligence ecosystem improves collective defense by alerting participating entities about new threats and vulnerabilities. Platforms like Information Sharing and Analysis Centers (ISACs), particularly the Health-ISAC, facilitate this exchange. Sharing data about attack signatures, phishing campaigns, and malware samples enables faster and more coordinated responses across the healthcare sector. Integration challenges in healthcare include maintaining patient privacy while sharing security data, ensuring interoperability between diverse technology systems, and overcoming resource constraints in smaller providers.(26) Addressing these challenges requires standardized threat intelligence formats (e.g., STIX and TAXII), privacy-preserving data sharing protocols, and ongoing training for healthcare cybersecurity staff. Frameworks embedding threat intelligence provide a proactive cybersecurity posture, enabling healthcare organizations not just to respond to attacks but to predict and prevent them by leveraging comprehensive, real-time threat insights.

## 6. Implementation Strategies and Best Practices

Adopting cybersecurity frameworks and effectively integrating threat intelligence within healthcare requires structured implementation strategies aligned with organizational goals, compliance needs, and operational realities. The process involves multiple steps and best practices:

**6.1.Risk Assessment:** The first step involves assessing the organization's current security posture and identifying critical assets such as patient records, medical devices, and administrative systems. Risk assessment frameworks evaluate vulnerabilities, threat likelihood, potential impacts, and existing controls. This assessment guides prioritization and resource allocation. Regular reassessment ensures adaptation to changing threats and technologies.(27)

**6.2.Policy Development:**
Effective cybersecurity frameworks require comprehensive policies addressing user access, data protection, incident response, vendor management, and employee training. Healthcare organizations develop policies tailored to regulatory mandates (HIPAA, GDPR) and industry best practices. Policies should be clear, enforceable, and updated regularly.(28)

**6.3.Resource Allocation:** Implementation demands appropriate funding, personnel, and technology investments. Cybersecurity teams in healthcare include security analysts, compliance officers, and IT specialists trained in medical technology environments. Budgets must accommodate tools such as firewalls, endpoint detection and response (EDR), secure communication protocols, and threat intelligence platforms.(29)

**6.4.Technical Measures:** Best practices advocate deploying a layered defense strategy. Key technical elements includes Zero Trust Architecture (ZTA): A paradigm shift from perimeter-based defense to continuous verification of users, devices, and network traffic regardless of location. ZTA enforces strict access controls, micro-segmentation, and least privilege principles, minimizing lateral movement opportunities for attackers. Multi-Factor Authentication (MFA): Enhances user identity verification by requiring multiple credentials (password and token, biometrics, etc.), reducing risks from compromised credentials, especially relevant in healthcare where insider threats and phishing are prevalent.(30) Encryption: Protects data in transit and at rest, ensuring confidentiality of sensitive health information even if intercepted or accessed unlawfully. Patch Management: Regularly updating medical devices, applications, and operating systems closes security gaps exploited by attackers.

**6.5.Continuous Threat Monitoring and Periodic Risk Assessments:** Ongoing monitoring through Security Information and Event Management (SIEM) systems enables real-time visibility into network and system activities. Regular vulnerability scans and penetration tests uncover emerging weaknesses.(31) Periodic risk assessments ensure the security posture adjusts to changes in technology, threat environment, and organizational processes.

These best practices reflect an integrated approach, combining organizational governance, technical controls, human factors, and collaboration to build resilience against healthcare cyber threats.

## 7. Challenges and Barriers

The healthcare industry faces significant challenges and barriers in implementing effective cybersecurity and threat intelligence frameworks due to the sector’s inherent complexity, evolving technology landscape, and regulatory environment.

### 7.1.Resource Limitations, Complexity, and Interoperability:

Healthcare organizations, especially smaller providers, often operate under constrained budgets with limited cybersecurity expertise and staffing. This resource scarcity hampers comprehensive security implementation and continuous monitoring efforts. The complexity of healthcare IT systems—comprising EHRs, legacy systems, IoMT devices, cloud services, and third-party applications—compounds these challenges. Interoperability issues persist due to the use of heterogeneous systems designed by different vendors, often lacking standard security protocols, which creates gaps exploitable by attackers. The push for system integration to improve patient care further increases attack surfaces, making consistent cybersecurity policies difficult to enforce across diverse platforms.(32) Moreover, the need to maintain system availability and usability for clinicians imposes constraints on deploying stringent security controls that might interfere with clinical workflows.

### 7.2.Vendor Risk, Compliance Gaps, and Legacy Systems:

Healthcare's dependency on a broad ecosystem of vendors introduces substantial supply chain risk. Third-party providers, including software vendors, cloud service suppliers, and device manufacturers, may have varying security postures, sometimes lagging behind in patching and vulnerability management. Vendor risk is frequently amplified by insufficient oversight and contractual cybersecurity requirements. Additionally, healthcare organizations often rely on legacy systems and medical devices with outdated security features or no longer supported patches.(33) These legacy assets become targets for attackers, as vulnerabilities persist unaddressed. Compliance gaps arise from fragmented regulations and uneven implementation across organizations, sometimes resulting in security practices that meet minimal legal requirements but fail to prevent real-world attacks robustly.

### 7.3.Ethical and Legal Issues with Threat Intelligence, Data Sharing, and AI:

Ethical and legal considerations significantly impact the use of threat intelligence and advanced technologies in healthcare cybersecurity. Sharing threat intelligence across organizations is critical for collective defense but raises privacy concerns, especially regarding patient data that might be inadvertently exposed in shared security information. Legal frameworks governing data sharing vary internationally, complicating cross-jurisdictional cooperation. The use of Artificial Intelligence (AI) in threat detection and response, while promising, introduces new dilemmas. AI models require large datasets, including sensitive health information, for training, raising questions about consent, data anonymization, and algorithmic bias.(34) There are also concerns about accountability when AI-driven decisions affect cybersecurity outcomes. Healthcare entities must navigate these challenges carefully to balance innovation with patient rights, legal compliance, and ethical standards.

## 8. Emerging Trends and Future Directions

Healthcare cybersecurity continues to evolve rapidly, with several emerging trends shaping the future of threat intelligence and defense frameworks.

### AI-Powered Threat Detection and Response:

Artificial Intelligence and machine learning represent the forefront of next-generation cybersecurity in healthcare. AI's ability to process and analyze massive datasets in real-time enables early identification of sophisticated threats, including zero-day vulnerabilities and advanced persistent threats (APTs).(35) AI-powered systems can enhance anomaly detection, automate incident response workflows, and prioritize alerts to reduce analyst workload and improve response timeliness. Predictive analytics within AI tools forecast emerging vulnerabilities based on threat actor behaviors, enabling proactive defense measures. In healthcare, AI is increasingly applied to monitor network traffic, safeguard IoMT devices, and detect subtle data exfiltration attempts hidden within legitimate activities.

### 8.1.Threat Intelligence Automation and Real-Time Incident Analysis:

Automation of threat intelligence gathering, correlation, and distribution accelerates the detection-to-response cycle. Real-time incident analysis platforms integrate continuously updated threat feeds from internal and external sources, employing AI to contextualize threats specific to healthcare environments. This shift towards automated and dynamic intelligence dissemination improves the agility and precision of cybersecurity operations.(36) Healthcare organizations benefit from streamlined workflows that reduce human error and enable rapid containment of attacks, critical in settings where delays can jeopardize clinical care.

### 8.2.Regulatory Changes and Novel Frameworks in Development:

With the increasing complexity and volume of cyber threats, regulators globally are revising standards and requirements for healthcare cybersecurity. Emerging policies emphasize not only data protection but also operational resilience and incident transparency. Novel frameworks designed to address AI governance, supply chain security, and integrated risk management are under development.(37) These frameworks aim to provide holistic and adaptive guidance to healthcare entities while addressing ethical, legal, and technical challenges posed by new technologies. The evolving regulatory landscape necessitates healthcare organizations to stay abreast of compliance requirements and adapt their cybersecurity strategies accordingly to mitigate legal risks and maintain patient trust.

## CONCLUSION

The digital transformation of healthcare has unlocked immense potential for enhancing patient care and operational efficiency but has also introduced significant cybersecurity vulnerabilities. As healthcare systems become increasingly complex and interconnected, protecting sensitive patient data and maintaining system availability are critical to ensuring both patient safety and trust. Cybersecurity threat intelligence frameworks offer a structured, evidence-based approach to mitigating these risks by integrating advanced technologies, continuous monitoring, and collaborative intelligence sharing. While challenges such as limited resources, outdated infrastructures, and ethical concerns around data use persist, emerging solutions—including AI-driven threat detection, automated response mechanisms, and evolving regulatory standards—present promising opportunities to strengthen resilience. Ultimately, building a proactive, adaptive, and collaborative cybersecurity culture anchored in robust frameworks is essential to defend healthcare systems against sophisticated threats while safeguarding the confidentiality, integrity, and availability of vital health information.

## REFERENCES

[1]. Stoumpos AI, Kitsios F, Talias MA. Digital Transformation in Healthcare: Technology Acceptance and Its Applications. Int J Environ Res Public Health. 2023 Feb 15;20(4):3407.
[2]. Aldosari B. Cybersecurity in Healthcare: New Threat to Patient Safety. Cureus. 2025 May 6;
[3]. Elendu C, Omeludike EK, Oloyede PO, Obidigbo BT, Omeludike JC. Legal implications for clinicians in cybersecurity incidents: A review. Medicine. 2024 Sep 27;103(39):e39887.
[4]. Javaid M, Haleem A, Singh RP, Suman R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications. 2023 Dec;1:100016.
[5]. Wang W, Ferrari D, Haddon-Hill G, Curcin V. Electronic Health Records as Source of Research Data. In 2023. p. 331–54.
[6]. Matthew P, Mchale S, Deng X, Nakhla G, Trovati M, Nnamoko N, et al. A Review of the State of the Art for the Internet of Medical Things. Sci. 2025 Mar 24;7(2):36.
[7]. Alexiuk M, Elgubtan H, Tangri N. Clinical Decision Support Tools in the Electronic Medical Record. Kidney Int Rep. 2024 Jan;9(1):29–38.
[8]. Li S, Surineni K, Prabhakaran N. Cyber-Attacks on Hospital Systems: A Narrative Review. The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice. 2025 Sep;7:30–9.
[9]. Priestman W, Anstis T, Sebire IG, Sridharan S, Sebire NJ. Phishing in healthcare organisations: threats, mitigation and approaches. BMJ Health Care Inform. 2019 Sep 4;26(1):e100031.
[10]. Saxena N, Hayes E, Bertino E, Ojo P, Choo KKR, Burnap P. Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. Electronics (Basel). 2020 Sep 7;9(9):1460.
[11]. Keskin OF, Caramancion KM, Tatar I, Raza O, Tatar U. Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. Electronics (Basel). 2021 May 13;10(10):1168.
[12]. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al. Healthcare Data Breaches: Insights and Implications. Healthcare. 2020 May 13;8(2):133.
[13]. Mahboubi A, Luong K, Aboutorab H, Bui HT, Jarrad G, Bahutair M, et al. Evolving techniques in cyber threat hunting: A systematic review. Journal of Network and Computer Applications. 2024 Dec;232:104004.
[14]. Das P, Asif MdR Al, Jahan S, Ahmed K, Bui FM, Khondoker R. STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Treatment of an In-Vehicle Infotainment System. Vehicles. 2024 Jun 30;6(3):1140–63.
[15]. Jada I, Mayayise TO. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data Inf Manag. 2024 Jun;8(2):100063.
[16]. Alaeifar P, Pal S, Jadidi Z, Hussain M, Foo E. Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. Journal of Information Security and Applications. 2024 Jun;83:103786.
[17]. Kioskli K, Grigoriou E, Islam S, Yiorkas AM, Christofi L, Mouratidis H. A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain. Int J Inf Secur. 2025 Apr 10;24(2):90.
[18]. The NIST Cybersecurity Framework (CSF) 2.0. 2024 Feb.
[19]. Edemekong PF, Annamaraju P, Afzal M, Haydel MJ. Health Insurance Portability and Accountability Act (HIPAA) Compliance. 2025.
[20]. Kitsios F, Chatzidimitriou E, Kamariotou M. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability. 2023 Mar 27;15(7):5828.
[21]. Tschider C, Compagnucci MC, Minssen T. The new EU–US data protection framework's implications for healthcare. J Law Biosci. 2024 Jul 7;11(2).
[22]. Antariksa MDS, Angin MP, Widodo AP. COBIT 2019 Framework in IT Governance: A Systematic Literature Review of Implementation Challenges and Benefits Across Various Industry Sectors. Journal of Renewable Energy, Electrical, and Computer Engineering. 2025 Mar 17;5(1):99–105.
[23]. Kaur R, Gabrijelčič D, Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 2023 Sep;97:101804.

[24]. Mahida A. Real-Time Incident Response and Remediation-A Review Paper. Journal of Artificial Intelligence & Cloud Computing. 2023 Jun 30;1–3.
[25]. Mohamed N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowl Inf Syst. 2025 Aug 30;67(8):6969–7055.
[26]. Luidold C, Jungbauer C. Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. Front Med (Lausanne). 2024 May 9;11.
[27]. Metin B, Duran S, Telli E, Mutlutürk M, Wynn M. IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture. Information. 2024 Jan 17;15(1):55.
[28]. Adebola Folorunso, Ifeoluwa Wada, Bunmi Samuel, Viqaruddin Mohammed. Security compliance and its implication for cybersecurity. World Journal of Advanced Research and Reviews. 2024 Oct 30;24(1):2105–21.
[29]. Ilca LF, Lucian OP, Balan TC. Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response. Sensors. 2023 Jul 28;23(15):6757.
[30]. Dakić V, Morić Z, Kapulica A, Regvart D. Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations. Journal of Cybersecurity and Privacy. 2024 Dec 30;5(1):2.
[31]. González-Granadillo G, González-Zarzosa S, Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors. 2021 Jul 12;21(14):4759.
[32]. He Y, Aliyu A, Evans M, Luo C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. J Med Internet Res. 2021 Apr 20;23(4):e21747.
[33]. Singh N, Buyya R, Kim H. Securing Cloud-Based Internet of Things: Challenges and Mitigations. Sensors. 2024 Dec 26;25(1):79.
[34]. Elendu C, Omeludike EK, Oloyede PO, Obidigbo BT, Omeludike JC. Legal implications for clinicians in cybersecurity incidents: A review. Medicine. 2024 Sep 27;103(39):e39887.
[35]. Kaur R, Gabrijelčič D, Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 2023 Sep;97:101804.
[36]. Alaeifar P, Pal S, Jadidi Z, Hussain M, Foo E. Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. Journal of Information Security and Applications. 2024 Jun;83:103786.
[37]. Singh K, Chatterjee S, Mariani M, Wamba SF. Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment. Technovation. 2025 May;143:103219.