ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

Cybersecurity Threats and Mitigation Strategies in Healthcare During the Covid-19 Pandemic: A Scoping Review

Itunu Omolade Dave-Agboola[1]*; Richard Kayode Alhassan[2]

Corresponding Author: Itunu Omolade Dave-Agboola*

Publication Date: 2026/04/18

Abstract:

- ***Introduction***

The COVID-19 pandemic unexpectedly accelerated the digital transformation of healthcare systems, exposing them to unprecedented cybersecurity risks. During the COVID-19 pandemic, the healthcare system was affected by ransomware, phishing, and other cyber threats which disrupted the delivery of healthcare services, compromised patient data, and challenged public health emergency response. Although the cyberthreats and cyberattacks were documented, there is a limited synthesis of lessons learned for pandemic preparedness.

- ***Methods***

Following the Arksey and O'Malley framework and PRISMA-ScR guidelines, we conducted a systematic search of peer-reviewed and grey literature published between January 2020 and December 2025 across PubMed, Scopus, Web of Science, IEEE Xplore, and Google Scholar. Eligible studies reported on cyber threats, mitigation measures, and impacts on healthcare or public health response during COVID-19. Data were extracted using a standardized template and analyzed descriptively and thematically, categorizing threats, mitigation strategies, and lessons learned.

- ***Results***

Twenty-six studies were included, comprising scoping/systematic reviews, empirical analyses, case studies, surveys, and policy reports. The most prevalent threats were ransomware and phishing, followed by malware, device/IoMT vulnerabilities, and data breaches. Impacts included service disruption, diagnostic delays, patient safety risks, and widespread data exposure. Mitigation strategies spanned technical (e.g., multi-factor authentication, segmentation, backups), organizational (e.g., incident response planning, workforce training), and policy/governance measures (e.g., reporting systems, cross-sector coordination). Key lessons highlighted the importance of layered socio-technical defenses, workforce preparedness, tested recovery plans, and integrated cyber governance. Major gaps were noted in the evaluation of mitigation effectiveness, and research on cyberbiosecurity and infodemic-related threats.

- ***Conclusions***

Health systems must adopt resilient, evidence-informed, socio-technical strategies to mitigate cyber threats, maintain continuity of care, and protect patient data. Policymakers should integrate cybersecurity into emergency planning, strengthen reporting and governance frameworks, and support research on intervention effectiveness and emerging threats.

Keywords: *Cybersecurity; Healthcare; Public Health; COVID-19; Pandemic Preparedness; Ransomware; Phishing; Mitigation Strategies; Scoping Review.*

How to Cite: Itunu Omolade Dave-Agboola; Richard Kayode Alhassan (2026) Cybersecurity Threats and Mitigation Strategies in Healthcare During the Covid-19 Pandemic: A Scoping Review. *International Journal of Innovative Science and Research Technology*, 11(4), 1105-1117. https://doi.org/10.38124/ijisrt/26apr799

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

I. INTRODUCTION: CYBERSECURITY IN HEALTHCARE

The healthcare sector has become increasingly reliant on digital technologies such as Electronic Health Records (EHRs), telehealth systems, and the Internet of Medical Things (IoMT) delivering major clinical and operational benefits while simultaneously expanding cyber-attack. Sensitive patient data and mission-critical systems make healthcare organizations highly attractive targets for cybersecurity threats. Between 2018 and 2022, the U.S. healthcare experienced a 278% increase in large-scale ransomware-related breaches, highlighting the escalating threat to patient safety and operational integrity (ASPR, 2023; Cycore Compliance, 2025). By 2025, over 92% of healthcare organizations reported being targeted by cyberattacks in the preceding year, with 90% experiencing at least one breach and ransomware-related downtime averaging 19 days per incident (Dialoghealth, 2025). These trends underscore the urgent need for robust and resilient cybersecurity frameworks across health systems.

The COVID-19 pandemic further amplified these vulnerabilities as healthcare systems underwent rapid digital transformation to sustain service delivery amid lockdowns and workforce disruptions. The swift expansion of remote work, telemedicine, and digital public health platforms, combined with limited staffing and strained IT infrastructure, created ideal conditions for cybercriminal exploitation (Muthuppalaniappan & Stevenson, 2021). Hospitals, public health agencies, laboratories, and vaccine research facilities were subjected to coordinated ransomware, malware, and phishing campaigns aimed at disrupting critical services and exfiltrating sensitive data (CISA, 2021). International organizations, including the World Health Organization (WHO) and INTERPOL, issued multiple warnings during the pandemic, noting a sharp rise in cyberattacks targeting health systems and cautioning that such attacks could delay patient care and compromise emergency response functions (WHO, 2024a). Empirical studies further confirm that cybersecurity risks during COVID-19 extended beyond financial losses to directly threaten healthcare delivery and public trust (He et al., 2021).

Despite the growing body of literature documenting healthcare cyber threats and mitigation measures, pandemic-specific lessons remain fragmented across technical, clinical, and policy domains, with limited systematic synthesis. This fragmentation constrains the ability of policymakers and health system leaders to draw integrated, evidence-based conclusions for future preparedness. A scoping review is therefore well suited to map the breadth and depth of existing evidence on cybersecurity incidents, response measures, and governance challenges during the COVID-19 pandemic. Through a systematic charting of the pandemic-era cybersecurity experiences, this review seeks to establish an evidence-based foundation for strengthening the resilience of healthcare and public health systems against future systemic digital threats.

➢ *Primary Objective*

To map and synthesize existing literature on cybersecurity challenges and strategies implemented during the COVID-19 pandemic in the context of public health response.

➢ *Secondary Objectives*

- Identify types of cyber threats targeting healthcare systems during COVID-19.
- Explore mitigation strategies and their effectiveness.
- Highlight gaps in preparedness and policy for future pandemics.

➢ *Research Questions*

- What types of cyber threats were prevalent in healthcare and public health during COVID-19 pandemic?
- Which cybersecurity mitigation strategies were implemented, and how effective were they?
- What lessons and best practices can guide future pandemic cybersecurity preparedness?

II. METHODS

This scoping review followed the methodological framework proposed by Arksey and O'Malley (2005), which outlines five key stages: identifying the research question, identifying relevant studies, study selection, charting the data, and collating, summarizing, and reporting results. The review also adhered to the PRISMA-ScR (Preferred Reporting Items for Systematic Reviews and Meta-Analyses Extension for Scoping Reviews) guidelines to ensure transparency and rigor in reporting (Tricco et al., 2018).

A. Eligibility Criteria

➢ *Inclusion Criteria*

- Studies that were published between January 2020 and December 2025.
- Peer-reviewed articles, reports, and relevant grey literature.
- Focus on cybersecurity incidents, challenges, or mitigation strategies in healthcare or public health during the COVID-19 pandemic.
- English language publications.

➢ *Exclusion Criteria*

- Cybersecurity studies unrelated to healthcare or public health
- Opinion pieces without empirical or policy relevance.
- Non-English publications.

B. Information Sources and Search Strategy

The search was conducted across multiple databases, including PubMed, Scopus, Web of Science, IEEE Xplore, and Google Scholar for grey literature. Filters will be applied for publication date (2020–2025) and language (English). The full search strategy for each database was documented. The search strategy used a combination of keywords and Boolean operators.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

➢ *Keywords and Boolean operators*

"cybersecurity" OR "cyber threats" OR "cyber-attacks" OR "data breach") AND ("COVID-19" OR "coronavirus" OR "pandemic") AND ("public health" OR "healthcare" OR "hospital" OR "health system."

➢ *Literature Search Terms*

The literature search was conducted using PubMed, Scopus, Web of Science, IEEE Xplore, and Google Scholar. Search terms included: "Cybersecurity" OR "cyber threats" OR "cyber-attacks" OR "data breach" AND "COVID-19" OR "coronavirus" OR "pandemic" AND "healthcare" OR "public health" OR "hospital" OR "health system".

Table 1: Literature Search Strategy

Database	Search terms	Limiters/Truncation/Boolean	Results
Pubmed	("cybersecurity" OR "cyber threats" OR "cyber-attacks" OR "data breach") AND ("COVID-19" OR "coronavirus" OR "pandemic") AND ("healthcare" OR "public health" OR "hospital" OR "health system")	Boolean operators (AND/OR); Date filter: (2020–2025); English language	38
Scopus	("cybersecurity" OR "cyber threats" OR "cyber-attacks" OR "data breach") AND ("COVID-19" OR "coronavirus" OR "pandemic") AND ("healthcare" OR "public health" OR "hospital" OR "health system")	Boolean operators (AND/OR); Date filter: (2020–2025); English language	26
Web of Science	("cybersecurity" OR "cyber threats" OR "cyber-attacks" OR "data breach") AND ("COVID-19" OR "coronavirus" OR "pandemic") AND ("healthcare" OR "public health" OR "hospital" OR "health system")	Boolean operators (AND/OR); Date filter: (2020–2025); English language	37
IEEE Xplore	("cybersecurity" OR "cyber threats" OR "cyber-attacks" OR "data breach") AND ("COVID-19" OR "pandemic") AND ("healthcare" OR "health system")	Boolean operators (AND/OR); Date filter: (2020–2025); English language	29
Google Scholar	("cybersecurity" AND "COVID-19" AND "healthcare") OR ("cyber threats" AND "pandemic" AND "public health")	Boolean operators (AND/OR); Date filter: (2020–2025); English language Grey literature	24

➢ *PICO Framework*

The PICO framework is a structured strategy to develop research questions and guiding evidence synthesis, especially in evidence-based practice (Eriksen & Frandsen, 2018). The framework assisted in systematically breaking down the research topic into four components: population/problem, intervention/exposure, comparator/control, and outcome. Table 2 below shows the PICO structure used for this scoping review.

Table 2: PICO Framework

Component	Definition
Population	Healthcare systems, public health institutions, hospitals, and health organizations operating during the COVID-19 pandemic.
Intervention/Exposure	Exposure to cybersecurity threats during the COVID-19 pandemic, including ransomware, phishing, malware, data breaches, and IoMT vulnerabilities; and implementation of mitigation strategies (technical, organizational, and policy measures).
Comparison	Pre-pandemic vs. pandemic cybersecurity landscape; or comparison across different mitigation approaches, settings, or levels of preparedness.
Outcome	Impact of cyber threats on healthcare delivery and public health response (e.g., service disruption, patient safety risks, data breaches), as well as effectiveness of mitigation strategies, lessons learned, and implications for future pandemic preparedness.

➢ *Study Selection Process*

This scoping review focused on literature published between January 2020 and December 2025 to capture evidence generated during the COVID-19 pandemic period. Only studies published in the English language were considered for inclusion. Articles without accessible full text were excluded from the review. Additionally, only studies with the capacity to address the research questions, as guided by the PICO framework, were included.

All retrieved records were screened by two independent reviewers to ensure consistency and reduce selection bias. Sources of evidence eligible for inclusion were identified from PubMed, Scopus, Web of Science, IEEE Xplore, and Google Scholar (for grey literature).

As this scoping review aimed to map cybersecurity threats, impacts, and mitigation strategies in healthcare and public health systems during the COVID-19 pandemic, all studies reporting relevant outcomes such as types of cyber threats (e.g., ransomware, phishing, malware), impacts on

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

healthcare delivery (e.g., service disruption, patient safety risks, data breaches), and implemented mitigation strategies (technical, organizational, or policy-level) were included. Full-text screening followed potentially relevant studies. Discrepancies were resolved through discussions and consultation.

The selection process is illustrated using a PRISMA flow diagram as shown in Figure 1 below:

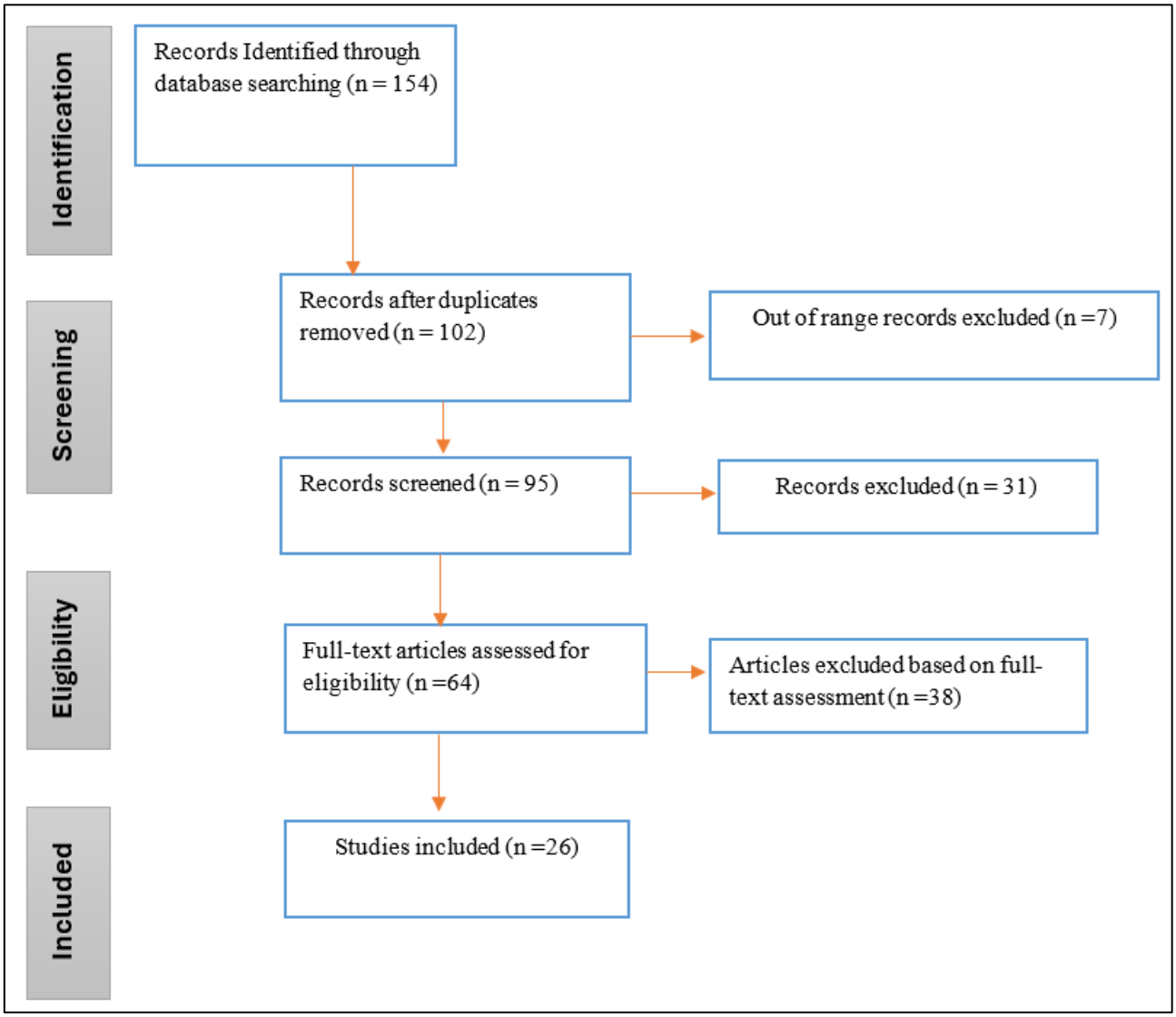

Fig 1. PRISMA Flow Diagram Depicting the Steps and Processes for Study Selection and Inclusion.

➢ *Data Extraction and Charting*

A standardized data extraction template was developed to capture the author(s), year, country/region, study type and design, type of cyber threat, impact on healthcare/public health response, mitigation strategies, lessons learned and recommendations from the selected studies. The data was charted in Excel for consistency and ease of analysis.

➢ *Data Analysis and Synthesis Approach*

The extracted data was synthesized using descriptive analysis and thematic analysis. Cyber threats were categorized, and mitigation strategies were grouped by technical, organizational, and policy measures. Lessons learned were summarized to identify gaps and inform future pandemic preparedness.

III. RESULTS

This scoping review identified and synthesized evidence from 26 selected sources examining cybersecurity threats, impacts, and mitigation strategies within healthcare and public health systems during the COVID-19 pandemic. The included studies comprised a diverse range of study designs, including systematic and scoping reviews, empirical observational studies, qualitative case studies, surveys, policy reports, and grey literature. Geographically, the evidence spanned multiple regions, with representation from North America, Europe, and global multi-country analyses. The extracted data were charted across key domains, including types of cyber threats, impacts on healthcare and public health response, mitigation strategies, and lessons learned.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

Table 3 below presents a structured summary of the key characteristics and findings of the included studies.

Table 3: Data Extraction

Author(s)	Year	Country/Region	Study Type and Design	Type of Cyber Threat	Impact on Healthcare/ Public Health Response	Mitigation Strategies	Lessons Learned and Recommendations
He et al.	2021	International	Scoping Review	Phishing, ransomware, malware, DDoS, IoMT vulnerabilities	Service disruption, data exposure risks, patient safety concerns	Patch management, segmentation, backups, workforce training, IR planning	Adopt socio-technical approaches, improve coordination
Chigada	2020	International	Systematic Review	Phishing, malware, ransomware, disinformation	Service disruptions, increased fraud, data compromise	Public awareness, law enforcement coordination	Expand empirical cyber impact studies
He et al.	2021	International	Scoping Review	Mixed cyber threats	Healthcare system vulnerabilities exposed	Risk management and workforce training	Standardization improves resilience
Neprash et al.	2022	USA	Empirical Observational Study	Ransomware	374 attacks, 42 million PHI exposed	Network segmentation, backups	Mandatory reporting improves preparedness
Muthuppalaniappan & Stevenson	2021	International	Perspective Review	Ransomware, phishing	Threatened global health operations	Governance strengthening	Global collaboration essential
CyberPeace Institute	2021	Global	Grey Literature Report	Ransomware, IP theft	45% increase in attacks	Coalition response	Strengthening global cooperation
INTERPOL	2020	Global	Law Enforcement Analysis	Phishing, malware, scams	Widespread cyber fraud	Public alerts	Public-private partnerships needed
CISA	2021	USA	Government Guidance	Ransomware, VPN exploits	Operational disruption risks	Multi-Factor Authentication, patching	Baseline cyber hygiene critical
WHO	2024	Global	Policy Brief	Cyberattacks & disinformation	Health system disruptions	Cyber capacity strengthening	Cyber into emergency preparedness
Al-Qahtani et al.	2022	International	Survey Review	Phishing	Surge in phishing attacks	Email filtering, training	Continuous adaptation required
Portela et al.	2023	Portugal	Economic Case Study	Ransomware	Loss of up to $7M per attack	Resilience investment	Proof of financial ROI
Georgiadou et al.	2021	Greece	Survey	Human-factor threats	Low staff awareness	Cybersecurity training	Culture change required
Gioulekas et al.	2022	Europe	Survey	Human & process threats	Variation in readiness	Standardized training	Uniform benchmarks recommended

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

Hoheisel	2023	International	Content Analysis	COVID-themed phishing	Increased sophisticatio n	Domain takedown	Continuous phishing monitoring
Rajput, et. al.,	2025	UK	Case Reports	Ransomware	Cancelled surgeries	Manual operations	Include cyber in continuity plans
Li	2025	International	Narrative Review	Ransomware, data breaches	Workflow collapse	Multi-layer defenses	Strengthen device security
Laith	2025	International	Conceptual Review	Cyberbiosecur ity threats	Genomic data risk	Access controls	Include cyberbiosecurity
Fox-IT	2023	Netherlands	Industry Whitepaper s	Ransomware	Weeks of downtime	IR playbooks	Operational readiness is critical
Papathanasiou, et al., 2023	2023	Greece	Sector Briefings	Ransomware, BEC	Sector-wide targeting	Policy coordination	Use threat intelligence
Chen, et. al.,	2021	International	Review	Multi-layer threats	Governance failures	Integrated controls	Holistic governance needed
Sabet, et al.	2024	International	Systematic Review	Network vulnerabilities	LMIC gaps	Standards	More LMIC research needed
Boven, et al.,	2024	Multi-country	Qualitative Study	Ransomware	Delayed care	Rapid recovery	Clinical contingency critical
Ewoh & Vartiainen	2024	International	Systematic Review	Ransomware, phishing	Governance failures	Sociotechnic al interventions	Whole-system governance
Klick et al.	2021	Germany	Vulnerabilit y Scan	Exposed hospital systems	32% vulnerable services	Patch updates	Reduce attack surface
Bloomberg	2023	Ireland	Case Study	Ransomware	Service cancellation s	Manual workflows	Workforce readiness critical

Table 4: Thematic Content Analysis of Included Studies

Themes	**Related Research Findibgs**
Prevalence and Types of Cyber Threats in Healthcare during COVID-19	He, et al., 2021 (International) • Reported multiple threats: ransomware, phishing, malware, Distributed Denial of Service, and Internet of Medical Things vulnerabilities. • Highlighted widespread service disruption and data exposure risks. Chigada, 2020. (International) • Identified phishing, malware, ransomware, and disinformation as dominant threats. • Noted increased cyber fraud and exploitation of pandemic-related fear. • INTERPOL, 2020 (Global) INTERPOL, 2020 (Global) • Documented global surge in phishing, scams, and malware campaigns targeting healthcare and the public. Al-Qahtani et al., 2022 (International) Significant rise in phishing attacks during the pandemic. Hoheisesel, 2023 (International) • COVID-themed phishing campaigns increased in sophistication and targeting.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

Ransomware as a dominant threat	Neprash et al., 2022 (USA) • Documented 374 ransomware attacks affecting ~42 million patient records. • Demonstrated large-scale impact on healthcare data security. Portela et al., 2023 (Portugal) • Estimated financial losses of up to $7 million per ransomware incident. CyberPeace Institute, 2021 (Global) • Reported 45% increase in ransomware attacks targeting healthcare. Rajput, et. al, 2025 (UK/Ireland) • Ransomware attacks led to cancelled surgeries and service shutdowns. Bloomberg, 2023 • Demonstrated prolonged disruption and reliance on manual systems.
Impact on healthcare delivery and public health response.	He et al., 2021 (International) • Cyber incidents caused service disruption, patient safety risks, and delayed care. Boven, et al., 2024 (Multi-country) • Reported delayed treatment and compromised clinical workflows. Rajput, et. al, 2025 (UK) • Highlighted cancellation of procedures and operational breakdown. Klick et al., 2021 (Germany) • Found 32% of hospital systems vulnerable, increasing risk of disruption. Li, 2025 (International). • Cyberattacks resulted in workflow collapse and reduced service delivery capacity.
Technical mitigation strategies	CISA, 2021 (USA) • Recommended multi-factor authentication, patch management, and secure VPN use. He et al., 2021 (International) • Emphasized segmentation, backups, and patching as core defenses. Fox-IT, 2023 (Netherlands) • Incident response playbooks and recovery systems reduced downtime. Klick et al., 2021 (Germany) • Highlighted importance of vulnerability scanning and patch updates. Hoheisel, 2023 (International) • Domain monitoring and takedown strategies reduced phishing risks.
Organisational and workforce-based strategies	Georgiadou et al., 2021 (Greece) • Identified low staff awareness as a key vulnerability. • Emphasized need for continuous cybersecurity training. Gioulekas et al., 2022 (Europe) • Reported variation in preparedness across institutions. • Recommended standardized training frameworks. Boven, et al., 2024 (Multi-country)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

	• Highlighted importance of clinical contingency planning and rapid recovery. Bloomberg 2023 • Demonstrated need for workforce readiness and manual fallback systems.
Policy and governance approaches	WHO, 2024 (Global) • Recommended integration of cybersecurity into emergency preparedness. CyberPeace Institute, 2021 (Global) • Emphasized global cooperation and information sharing. Papathanasiou, et al., 2023 (Greece) • Highlighted importance of sector-wide policy coordination and threat intelligence. Ewoh & Vartiainen, 2024 (International) • Advocated whole-system governance and sociotechnical interventions. INTERPOL, 2020 (Global) • Promoted public-private partnerships in cyber response.
Emerging Threats: Cyberbiosecurity and Data Risks	Laith, 2025 (International) • Identified risks to genomic data, biobanks, and laboratory systems. WHO, 2024 (Global) • Highlighted convergence of cyber threats and disinformation. Muthuppalaniappan & Stevenson, 2021 (International) • Noted cyber threats as broader risks to global health security.
Preparedness gaps and system weaknesses	Sabet, et al., 2024 (International) • Identified limited cybersecurity capacity in LMICs. Georgiadou et al., 2021 (Greece) • Highlighted human-factor vulnerabilities. Li, 2025 (International) • Emphasized insufficient device and system security. Chen, et al., 2021 (International) • Identified governance failures and lack of integration.
Lessons learnt for pandemic preparedness	He et al., 2021 (International) • Recommended socio-technical approaches and improved coordination. Ewoh & Vartiainen, 2024 (International) • Emphasized whole-system governance. WHO, 2024 (Global) • Advocated integration of cybersecurity into emergency planning. Fox-IT, 2023 (Netherlands) • Highlighted importance of operational readiness and tested recovery plans. CyberPeace Institute, 2021 (Global) • Reinforced need for global collaboration and resilience frameworks.

➢ *Thematic Analysis and Data Synthesis*

Twenty-six studies were included and charted across the domains of this scoping review. The body of evidence was heterogeneous in design and purpose, with a substantial portion comprised of reviews and sector reports and several empirical analyses and qualitative case studies documenting the operational impacts breached cybersecurity.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

DESCRIPTIVE FINDINGS

Key descriptive findings across the 26 studies included in this scoping review include:

- Most frequently reported threat: Ransomware which was explicitly mentioned in 14/26 records (=54%).
- Other common threats: Phishing/social engineering (=9/26, 35%), malware (=4/26, 15%), device/IoMT and network vulnerabilities (=3/26, 12%), and data exposure/breach/IP theft referenced in multiple reports (=4/26, 15%).
- Operational impacts: (8/26, 31%) studies/reports explicitly documented severe operational consequences during incidents (service cancellations, diverted patients, multi-week downtimes, workforce disruption, or quantifiable patient-data exposure). Notable quantified examples include Neprash et al. (2022): 374 ransomware attacks (2016–2021) with approximately 42 million patient records exposed, and Klick et al. (2021) that submitted an empirical scan showing that approximately 32% of analyzed services were vulnerable in German clinical entities.
- Geographic spread: Evidence was concentrated in North America and Europe and in multi-country/global reports. There was a dearth of empirical studies from Low- and Middle-Income Countries.

➢ *Emerging Themes from the Scoping Review*

The findings of this scoping review are grouped into three broad, cross-cutting themes that directly address the review questions: Types of cyber threats, Mitigation strategies (technical, organizational, policy), and Lessons learned / preparedness gaps.

➢ *Types of Cyber Threats*

- Ransomware: Dominant theme across reviews, empirical studies, industry analyses and case reports. Reported impacts included complete or partial EHR downtime, cancelled procedures, and long recovery periods.
- Phishing / social engineering: Increased volume and sophistication during the pandemic; many studies documented COVID-themed lures targeting both staff and the public.
- Malware and DDoS: Reported but less frequent in the selected set than ransomware/phishing.
- Device/IoMT and network vulnerabilities: Recurrent in systematic reviews and vulnerability scans; exposed internet-facing services and poorly configured medical devices were noted.
- Data exfiltration / IP theft / supply-chain attacks / disinformation: Appeared across sector reports and policy notes, with particular concern for research data (vaccine/ genomic data) and the compounding effect of disinformation on public health response.

➢ *Mitigation Strategies*

- Technical Strategies
- Network segmentation and least-privilege access: Dividing networks into isolated segments limits attackers' lateral movement, while restricting user permissions ensures individuals can only access systems necessary for their role.
- Regular patch management and vulnerability scanning: Systematic updating of software and proactive scanning for vulnerabilities reduces exposure to known exploits and strengthens overall system security.
- Off-site backups and tested restoration procedures: Storing backup data off-site and regularly testing restoration ensures rapid recovery from ransomware or system failures without data loss.
- Multi-factor authentication (MFA) and hardening of remote access (VPN) services: Adding multiple layers of verification and securing remote connections protects accounts and networks from unauthorized access.
- Domain monitoring and takedowns for phishing campaigns: Continuously tracking domain activity and taking down fraudulent sites reduces the risk of staff or patients falling victim to phishing attacks.

➢ *Organizational measures*

- Incident response (IR) playbooks, tabletop exercises, and simulation drills: Predefined IR playbooks, combined with simulated exercises, allow organizations to practice coordinated responses to cyber incidents and identify gaps before real attacks occur.
- Workforce capacity building: Regular staff training, phishing simulations, and integrating cybersecurity into organizational culture enhance awareness and reduce human-factor vulnerabilities that could be exploited by attackers.
- Business continuity plans with cyber scenarios and manual fallback workflows: Incorporating cyberattack scenarios into continuity planning ensures that critical healthcare operations can continue, even when digital systems are compromised, by using alternative manual processes.

➢ *Policy and governance measures*

- National/regional information-sharing mechanisms and incident reporting: Establishing structured channels for sharing cyber threat intelligence and reporting incidents enables timely alerts, coordinated responses, and improved situational awareness across the healthcare sector.
- Cross-sector coordination and prioritization of healthcare: Collaboration between healthcare organizations, law enforcement, and Computer Emergency Response Teams (CERTs), along with recognizing healthcare as critical infrastructure, strengthens preparedness and rapid response to cyber incidents.
- Legal/regulatory attention to devices, supply-chain security, and research data protection (cyberbiosecurity): Implementing policies and regulations ensures secure medical devices, resilient supply chains, and protection of sensitive research and genomic data, reducing vulnerabilities in healthcare and life sciences.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

➢ *Lessons Learned from Mitigation Strategies and Preparedness Gaps*

- Layered, socio-technical defenses are essential: Combining technical controls (Multi-Factor Authentication, network segmentation, patching, backups) with organizational measures (training, incident response playbooks) significantly reduces vulnerability to attacks.
- Workforce preparedness is critical: Regular staff training, phishing simulations, and embedding cybersecurity awareness into organizational culture are effective at mitigating human-factor risks.
- Incident response and recovery planning saves operational continuity: Predefined IR playbooks, tabletop exercises, and manual fallback workflows help healthcare systems respond quickly and maintain essential services during cyber incidents.
- Policy and governance measures enhance resilience: National and regional information-sharing, mandatory/voluntary reporting, cross-sector coordination, and prioritization of healthcare in cybersecurity strategies improve situational awareness and response speed.
- Technical measures must be tested and maintained: Off-site backups, tested restoration procedures, secure VPNs, and domain monitoring are most effective when regularly updated and actively managed.

➢ *Preparedness Gaps Identified*

- Limited empirical evaluation of effectiveness: Most mitigation measures are recommended or implemented without strong evidence quantifying their real-world impact during cyber incidents.
- Geographic and resource disparities: Evidence and preparedness strategies are heavily skewed toward high-income countries, with LMICs underrepresented and potentially more vulnerable.
- Emerging cyberbiosecurity risks: Protection of genomic data, biobanks, and laboratory systems is still underdeveloped in policy and practice.
- Under-addressed integration with public health emergencies: Cybersecurity is often siloed from broader pandemic preparedness and emergency planning, reducing system-wide resilience.
- Lack of standardized metrics: There is no uniform way to measure the impact of cyber incidents on healthcare operations, patient safety, or economic losses, hindering cross-study comparisons and policy evaluation.
- Practical implications
- For health system leaders: Prioritize tested incident response playbooks, regular backups and restoration exercises, staff training, and inclusion of cyber scenarios in business continuity planning.
- For policymakers: Mandate or incentivize standardized incident reporting, prioritize funding for cyber resilience (particularly for smaller providers), and integrate cyber risk into national health emergency plans.
- For researchers: Conduct rigorous, context-sensitive evaluations of mitigation measures, fill geographic evidence gaps, and develop standard outcome metrics for cyber incidents in health settings.

IV. DISCUSSION

➢ *Interpretation of Findings*

This scoping review provides a comprehensive synthesis of evidence on cybersecurity threats, mitigation strategies, and system-level lessons that emerged during the COVID-19 pandemic. The findings demonstrate that ransomware and phishing were the most prevalent cyber threats, consistently reported across empirical studies, reviews, government advisories, and sector intelligence reports. These attacks produced significant operational consequences, including service disruptions, delayed patient care, loss of diagnostic capacity, and large-scale exposure of sensitive patient data (Neprash et al., 2022; Portela et al., 2023; WHO, 2024). The pandemic context—characterized by workforce shortages, rapid digitalization, and overreliance on remote access technologies—created a highly permissive environment for cyber exploitation (CISA, 2021; Muthuppalaniappan & Stevenson, 2021).

Mitigation strategies documented across the literature clustered into technical, organizational, and policy/governance domains. Technically, multi-factor authentication, patch management, network segmentation, and secure backups emerged as baseline controls (CISA, 2021; He et al., 2021). Organizational responses emphasized incident response preparedness, staff cybersecurity training, and business continuity planning with manual fallback systems (Georgiadou et al., 2021; Boven, et al., 2024). At the policy level, strengthening national reporting systems, cross-sector intelligence sharing, and prioritization of healthcare as critical infrastructure were repeatedly recommended (CyberPeace Institute, 2021; WHO, 2024). However, despite broad agreement on best-practice controls, empirical evidence evaluating the real-world effectiveness of these interventions remains limited, highlighting a major translational gap between guidance and measurable outcomes.

➢ *Comparison with Existing Literature*

The findings of this review are highly consistent with previous systematic and narrative reviews conducted during the early and mid-phases of the pandemic. He et al. (2021) similarly identified ransomware, phishing, and insecure medical devices as dominant threat vectors and emphasized the need for layered technical and human-centered defenses. Chigada (2020) also reported a sharp rise in phishing and malware campaigns exploiting COVID-19 fears, reinforcing the social engineering dimension observed in this review.

Quantitative findings from Neprash et al. (2022) provide important empirical validation for the scale of the problem, documenting 374 ransomware attacks on U.S. hospitals and clinics with approximately 42 million patient records exposed. These figures align with the operational disruptions described in European contexts, including national health system shutdowns in Ireland and the United Kingdom (Portela et al., 2023; HSE Case Reports, 2023). Similarly, Klick et al. (2021) demonstrated that 32% of German hospital services were vulnerable through exposed internet-facing

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

systems, underscoring the structural nature of health system cyber risk beyond any single national context.

Beyond direct cyberattacks, this review also aligns with emerging literature on cyberbiosecurity and disinformation risks, which emphasize that biological data infrastructure, genomic research, and public-health messaging systems are increasingly vulnerable to both cyber espionage and information warfare (Laith, 2025; WHO, 2024). This convergence of cyberattacks and infodemics extends earlier work by Muthuppalaniappan and Stevenson (2021), who warned that cyber threats during pandemics represent not only technical risks but also strategic threats to global health security and public trust.

➢ *Implications for Policy and Practice*

The findings of this review have several critical implications for health security policy and healthcare delivery systems. First, cybersecurity must be institutionalized as a core component of pandemic preparedness and health emergency planning, rather than treated as a purely technical or IT-level concern. National preparedness frameworks should explicitly integrate cyber-incident scenarios into emergency response simulations and continuity-of-operations planning (CISA, 2021; WHO, 2024).

Second, healthcare organizations must move beyond compliance-based cybersecurity toward resilience-based models that prioritize rapid recovery, workforce readiness, and service continuity. Case studies demonstrate that even well-resourced systems experienced prolonged downtime and clinical disruption in the absence of tested backup and manual workflows (Portela et al., 2023; Boven, et al., 2024). Regular tabletop exercises, workforce phishing simulations, and interdisciplinary incident response teams should therefore be standard practice.

Third, policymakers should strengthen mandatory or incentivized cyber-incident reporting to improve real-time surveillance, cross-sector learning, and public accountability. Neprash et al. (2022) and the CyberPeace Institute (2021) both emphasize that under-reporting of incidents hampers accurate risk assessment and delays coordinated response. Finally, cyberbiosecurity governance must be urgently expanded to protect laboratory automation, genomic databases, biobanks, and vaccine research infrastructure, which are increasingly integral to global public health preparedness (Laith, 2025).

➢ *Gaps and Future Research Directions*

Despite the growing volume of literature, this review identified critical and persistent evidence gaps. First, there is a scarcity of rigorous outcome-based evaluations of cybersecurity interventions in healthcare. Most recommendations are derived from expert opinion, descriptive reports, or post-incident narratives rather than controlled or quasi-experimental impact studies.

Secondly, low- and middle-income countries (LMICs) remain underrepresented in the empirical cybersecurity literature, despite often having weaker digital infrastructure and fewer cyber resilience resources (Sabet, et al., 2024). This creates a structural knowledge gap that limits the generalizability of current best-practice guidance.

Thirdly, the intersection between cybersecurity and health misinformation/disinformation remains insufficiently explored, even though WHO (2024) has identified this convergence as a critical threat to emergency response effectiveness. Future research should also prioritize supply-chain cyber risk, medical device security, and genomics data protection, which are emerging but weakly regulated domains.

Finally, there is a need for standardized metrics for cyber incident impact in healthcare, including comparable indicators of downtime, patient harm, service delays, and economic losses, to strengthen global surveillance and evidence-based policy design.

➢ *Limitations*

First, the evidence base is heterogeneous, including reviews, empirical studies, grey literature, policy briefs, and case reports, which limit comparability and the ability to synthesize quantitative outcomes. Second, there is a geographic bias toward high-income countries, with limited representation from low- and middle-income settings, which may reduce the generalizability of the conclusions to resource-constrained healthcare systems. Finally, the review was restricted to English-language publications which may have excluded relevant non-English research on healthcare cybersecurity.

V. CONCLUSION

This scoping review highlights the significant cyber threats faced by healthcare and public health systems during the COVID-19 pandemic, with ransomware and phishing as the most prominent threats. The review emphasizes the critical operational and patient safety impacts of cyber incidents, while also mapping the technical, organizational, and policy-oriented mitigation strategies implemented across different contexts. Key lessons include the importance of layered socio-technical defenses, workforce training, tested incident response plans, and cross-sector collaboration. However, gaps remain, particularly in empirical evaluation of intervention effectiveness, representation of low-resource settings, and emerging domains such as cyberbiosecurity and infodemic-related risks. To enhance future pandemic preparedness, healthcare organizations and policymakers should integrate cybersecurity into emergency planning, adopt resilient governance frameworks, and prioritize evidence-based evaluation of mitigation strategies. These measures are essential to protect health systems, safeguard patient data, and maintain continuity of care in the face of evolving cyber threats.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

REFERENCES

[1]. Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. IET Information Security, 16(5), 324-345.

[2]. Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. International Journal of Social Research Methodology, 8(1), 19–32.

[3]. ASPR. (2023). Healthcare sector cybersecurity. U.S. Department of Health & Human Services. Retrieved from https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf.

[4]. Bloomberg (2023). *Case study of ransomware attack on Irish health services*. Available at https://www.bloomberg.com/news/features/2023-02-03/ireland-hospital-ransomware-attack-fractured-hacker-group-conti

[5]. Boven, L. S., Kusters, R. W., Tin, D., van Osch, F. H., De Cauwer, H., Ketelings, L., ... & Barten, D. G. (2024). Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals. *Annals of emergency medicine*, *83*(1), 46-56.

[6]. Chigada, J. (2020). Cyberattacks and threats during COVID-19: A systematic literature review. Journal of Cybersecurity, 6(1), 1–14.

[7]. Chen, J., Mohamed, M. A., Dampage, U., Rezaei, M., Salmen, S. H., Obaid, S. A., & Annuk, A. (2021). A multi-layer security scheme for mitigating smart grid vulnerability against faults and cyber-attacks. *Applied Sciences*, *11*(21), 9972.

[8]. CISA. (2021, January). Cybersecurity perspectives: Healthcare and public health response to COVID-19. Cybersecurity and Infrastructure Security Agency. Retrieved from https://www.cisa.gov/sites/default/files/publications/CISA_01132021_HPH_Factsheet_508.pdf

[9]. CyberPeace Institute. (2021). Cyber incidents affecting the healthcare sector during COVID-19. Retrieved from https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare-ExecSummary.pdf

[10]. Cycore Compliance. (2025). Healthcare in cybersecurity: Trends, threats, and solutions. Retrieved from https://www.cycoresecure.com/blogs/healthcare-cybersecurity-trends-threats-solutions

[11]. Dialoghealth. (2025). 120+ latest healthcare cybersecurity statistics for 2025. Retrieved from https://www.dialoghealth.com/post/healthcare-cybersecurity-statistics.

[12]. Eriksen, M. B., & Frandsen, T. F. (2018). The impact of patient, intervention, comparison, outcome (PICO) as a search strategy tool on literature search quality: a systematic review. Journal of the Medical Library Association, 106(4), 420–431.

[13]. Ewoh, O., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: A systematic review. Health Informatics Journal.

[14]. Fox-IT (2022). Understanding the impact of ransomeware on patient response. Do we know enough? Available at https://www.fox-it.com/be/understanding-the-impact-of-ransomware-on-patient-outcomes-do-we-know-enough/.

[15]. Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Hospitals' cybersecurity culture during the COVID-19 crisis. Information & Computer Security.

[16]. Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., ... & Ntanos, C. (2022, February). A cybersecurity culture survey targeting healthcare critical infrastructures. In *Healthcare* (Vol. 10, No. 2, p. 327). MDPI.

[17]. He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: A scoping review. Journal of Medical Internet Research, 23(4), e21747.

[18]. Hoheisel, R., van Capelleveen, G., Sarmah, D. K., & Junger, M. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, *128*, 103158.

[19]. INTERPOL (2020). Annual Report 2020. *Global law enforcement analysis of cyber fraud and scams*. Available at https://www.interpol.int › content › download

[20]. Klick, J., Brandstetter, T., et al. (2021). Epidemic? The attack surface of German hospitals during the COVID-19 pandemic. Computer Security Journal.

[21]. Laith, A. E. (2025). Addressing cyberbiosecurity challenges in the life sciences. Journal of Global Biosecurity.

[22]. Li, S., Surineni, K., & Prabhakaran, N. (2025). Cyber-attacks on hospital systems: A narrative review. *The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice*, *7*, 30-39.

[23]. Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. International Journal for Quality in Health Care, 33(1), mzaa117.

[24]. Neprash, H. T., et al. (2022). Trends in ransomware attacks on US hospitals and clinics, 2016–2021. JAMA Health Forum.

[25]. Papathanasiou, A., Liontos, G., Liagkou, V., & Glavas, E. (2023). Business email compromise (BEC) attacks: threats, vulnerabilities and countermeasures—a perspective on the Greek landscape. Journal of Cybersecurity and Privacy, 3(3), 610-637.

[26]. Portela, D., et al. (2023). Economic impact of a hospital cyberattack in a national context. Health Policy and Technology.

[27]. Rajput, K., Darzi, A., & Ghafur, S. (2025). Overlooked and under-reported: the impact of cyberattacks on primary care in the UK National Health Service. *The Lancet Digital Health*, *7*(7).

[28]. Tricco, A. C., Lillie, E., Zarin, W., et al. (2018). PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation. Annals of Internal Medicine, 169(7), 467–473.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr799

[29]. Sabet, C., Lin, J. C., Zhong, A., & Nguyen, D. (2024). Cybersecurity in the age of digital pandemics: protecting patient data in low-income and middle-income countries. *The Lancet Global Health*, *12*(6), e911-e912.

[30]. World Health Organization. (2024). WHO reports outline responses to cyber-attacks on health care and the rise of disinformation in public-health emergencies. Retrieved from https://www.who.int/news/item/06-02-2024-who-reports-outline-responses-to-cyber-attacks-on-health-care-and-the-rise-of-disinformation-in-public-health-emergencies