The Review Of
DIABETIC
STUDIES OPEN ACCESS

The Role Of Nursing In Cybersecurity Management In Digital Healthcare Environments: A Systematic Review

Amal Mohammed A. Hamdi[1] , Mousa Essa Ibreaheem Haqawi[2] Abdulaziz Hamoud Al-Shehri[3] , Nora Mohammed Alqahtani[4], Taghreed Alhumaidi Abdullah Alanazi[5], Essa Mohammed Hagawe[6] , Yahya Mousa Alhaqwi[7] , Ariaf Fleah Alanazi[8], Manar Nawar Almatrafi[9], Rehab Mohammed[10], Laila Hassan Asiri[11], Najla Hassan Alshehri[12], Essa Ali Washily[13], Rajaa Hussain Taliby[13]

[1]Aseer Health Cluster.
[2]Damad General Hospital
[3]Balsamer General Hospital.
[4]Khamis Mushait Hospital Centre.
[5]Alghadeer Primary Health Care Centre, 2nd Riyadh Health Cluster.
[6]Alreath General Hospital.
[7]Alreath General Hospital.
[8]North Border Health Cluster – Cardiac Center.
[9]Umm Al-Qura University Medical Clinic, Makkah.
[10]Aljouf Health Cluster.
[11]Primary Health Care Aljarf.
[12]General Department of Organizational Excellence.
[13]Alreath General Hospital.
Branch of the Ministry of Health, Riyadh Region.

Abstract

Background: The increasing digitization of healthcare has amplified cybersecurity threats, placing patient safety and data privacy at risk. Nurses, as frontline caregivers and primary users of electronic health records (EHRs), play a critical role in maintaining cybersecurity hygiene. However, the nursing profession remains underrepresented in formal cybersecurity protocols, training, and governance structures within healthcare systems.

Aim: This systematic review aims to explore the role of nursing in cybersecurity management within digital healthcare environments, highlighting how nurses contribute to cyber defense, the challenges they face, and strategies to strengthen their capacity in this evolving domain.

Method: A systematic review was conducted using five databases, such as PubMed, CINAHL, Scopus, ScienceDirect, and Google Scholar, targeting studies published between 2021 and 2025. Ten primary articles were selected based on predefined inclusion and exclusion criteria. PRISMA guidelines were followed, and quality appraisal was performed using a structured matrix.

Results: Seven core themes emerged: nurse training and education, technological integration, institutional policy inconsistencies, human factor vulnerabilities, interdisciplinary collaboration, preparedness through simulations, and digital infrastructure security. While most studies emphasized the rising importance of nursing in cyber readiness, they also revealed a lack of standardized education and limited involvement of nurses in policy development. Nurses expressed willingness to engage more deeply in cybersecurity initiatives when adequately trained and supported.

Conclusion: Nurses are critical to cybersecurity resilience in digital health. Strengthening their role through targeted education, policy inclusion, and interdisciplinary collaboration can significantly reduce cyber risks and enhance patient safety.

Keywords: Nursing, Cybersecurity, Digital Health, Information Security, Healthcare Policy, Electronic Health Records, Patient Safety, Nursing Education.

Introduction

Healthcare has undergone a digital transformation, with the advent of electronic health records (EHRs), telemedicine, and the Internet of Medical Things (IoMT), which significantly improve patient care and operational efficiency (Sharma, 2023; Baptist et al., 2023). However, these developments also have a two-edged sword effect on increasing the cyber-attack surface, and making healthcare one of the most targeted industries by cybercriminals (Sharma, 2023). Healthcare organizations today handle enormous amounts of sensitive patient information across interconnected systems, and this creates appealing possibilities to exploit for attackers while creating complicated vulnerabilities to protect (Baptist et al., 2023). Therefore, cybersecurity has emerged as a key issue in digital health, with threats such as ransomware, data breaches, and phishing attacks looming large over clinical operations (Awobelem et al., 2025). In the current era, where the networked devices and the data-driven workflows have pervaded the modern hospital, an attack on the system will compromise the integrity, confidentiality, and availability of critical healthcare information, disrupting the continuity of care (Ali & Mijwil, 2024).

The importance of cybersecurity in healthcare is highlighted by the potentially devastating impact of cyberattacks on patient safety, privacy, and trust. Privacy violations, identity theft, financial losses, regulatory fines, and irreversible damage to the reputation of healthcare institutions can be the result of breaches of patient information (Nasrabadi et al., 2024). Cyberattacks have disrupted hospital operations and even jeopardized lives; the hospital ransomware attacks have led to postponing surgeries and diverting patients, clearly demonstrating the impact of a security breach on patient care (Awobelem et al., 2025). In addition to legal and financial ramifications, a significant data breach is often followed by patient trust and public confidence in digital healthcare services in the long run (Nasrabadi et al., 2024; Wright, 2023). As a result, robust cybersecurity has become acknowledged as a pillar for patient welfare protection and the sustainability of contemporary healthcare systems (Alotaibi et al., 2022; Alruwaili et al., 2022; Shubayra et al., 2022).

Given such a high risk, clinical frontline healthcare workers - primarily nurses - are critical to cybersecurity initiatives. Nurses make up the largest percentage of the healthcare workforce, and often form the team that manages electronic patient information and interacts with health IT systems on a day-to-day basis. As such, they are on the front lines of protecting sensitive data in hospitals and clinics (Nasrabadi et al., 2024). Protecting patient information is not only a legal and ethical obligation for nurses but is also necessary to ensure the trust between patients and providers (Nasrabadi et al., 2024). Current healthcare guidelines focus on the importance for nurses to follow strict privacy rules (e.g. HIPAA) and implement safeguards, including strong passwords, access controls, encryption, and careful monitoring for suspicious activity, as part of routine practice (Abbasi & Smith, 2024). For example, it is anticipated that nurses should have good "cyber hygiene" - regularly updating credentials, recognizing phishing attempts, and following data access protocols - to minimize the risk of breaches (Nasrabadi et al., 2024). Through careful adherence to cybersecurity best practices and engagement in organizational security efforts, nurses can greatly minimize the vulnerabilities of the human factor and play an active role in the protection of health information (Pears & Konstantinidis, 2021; Abbasi & Smith, 2024).

Nonetheless, new challenges highlight the importance of better supporting and defining the nursing role in cybersecurity. Nurses have particular challenges in practice when attempting to safeguard patient data. Firstly, the landscape of cyber threats is constantly evolving and nurses must keep their knowledge updated and be vigilant to new methods of attack (Nasrabadi et al., 2024). Human elements are often the weakest link in security: lack of cybersecurity awareness and training among healthcare staff has been cited as major security vulnerabilities in healthcare systems (Awobelem et al., 2025; Sharma, 2023). Nurses also need to balance the need for quick access to information for patient care with the need to ensure strict privacy and security - a tension that can be challenging to balance amidst the demands of clinical work

(Nasrabadi et al., 2024). In addition, the integration of new technologies and IoMT devices into care has added more complexity and potential security gaps that nurses must be aware of (Layode et al., 2024; Nasrabadi et al., 2024). Even the most sophisticated technical defenses are susceptible to user errors or insider threats, so allowing nurses improved cybersecurity education, clear policies, and inclusion in cybersecurity governance is increasingly recognized as necessary (Pears & Konstantinidis, 2021; Alharbi & Alkhalifah, 2024).

Despite increasing awareness of these problems, the role that nursing can play in management of cybersecurity is an under-examined field that requires thorough investigation. Most studies and reviews examine healthcare cybersecurity at a broad level and point to the roles that staff training, organizational culture, and technology integration play in critically impacting security outcomes (Alharbi and Alkhalifah, 2024; Layode et al., 2024). However, there is an urgent need to synthesize evidence that is focused on nurses, who are the bridge between clinical practice and cybersecurity implementation. A dedicated systematic review on this topic is therefore warranted to fill that gap. This review will collate current knowledge of the contribution of nurses to cybersecurity in digital healthcare environments, key challenges and best practices, and areas for improvement (Alruwaili et al., 2023; Alqarni et al., 2023; Alsaedi et al., 2022; Matmi et al., 2023). By bringing together information from the nursing perspective, the purpose of the review is to educate healthcare leaders and policymakers on how to strengthen cybersecurity through the use of nursing practice - ultimately contributing to the protection of patient data and trust in an era of digital healthcare.

Problem Statement

While digitalization has greatly improved patient care, the rapid digitalization of healthcare has also put hospitals and clinics at unparalleled risk of cybersecurity threats. Electronic health records, connected medical devices, and telehealth are now part of care delivery - and each represents vulnerabilities that cyber attackers take advantage of. The healthcare industry is therefore becoming a target for frequent data breaches and ransomware attacks, resulting in the compromise of patient information, loss of services, financial losses, and even patient safety risks. One of the most important reasons for this is that many cyber-attacks are a result of human factors: poor staff training, lack of cybersecurity awareness, and improper digital habits have made healthcare organizations particularly vulnerable. Nurses, especially, are at the frontline of digital healthcare - they routinely work with sensitive patient information, use connected clinical systems and manage care via electronic means. In contrast, only 22.7% of non-IT healthcare personnel (including nurses) feel that they are sufficiently trained in cybersecurity measures. The gap between the increasing threat to cybersecurity and the poor state of cybersecurity awareness among nursing personnel highlights an important issue: the role of nursing in the safeguarding of data and systems is not clearly defined or supported in many healthcare organizations. As a result, the behaviors or accidental mistakes of the frontline caregivers can become access points for cyberattacks. To address this problem, it is crucial to identify and bolster the role of nurses in cybersecurity management to ensure that patient care is safe and secure in the digital age.

Significance of the Study

Patient data security is just as important as patient security in today's digital healthcare. Cyber incidents such as data breaches or system outages not only put information at risk - they can put patient safety at risk by disrupting clinical services and undermining confidence in the healthcare system. Because nurses are the only healthcare professionals with a professional duty to protect patient privacy and safety, they are in the front line of defense against these dangers. By focusing on patient information security, nurses not only maintain confidentiality, but also ensure the integrity and availability of care delivery in an era of connected technology. However, cybersecurity in the healthcare sector is not just a technical challenge; it requires human vigilance and a culture of security. Studies confirm that employee behavior and awareness are key to an organization's cybersecurity posture, particularly as it is only one click away to open a phishing email or one weak password to cause a significant breach. This makes the empowerment of nurses through cybersecurity education and clear protocols a patient safety issue. Indeed, involving healthcare staff in cyber security has been recognized as an important approach to avoid "severe consequences, including patient harm or even death" that may occur due to cyberattacks.

In the broader digital healthcare context, this study is important as it highlights a relatively unnoticed aspect of the nursing practice. As the healthcare field across the world continues to invest in electronic records, telehealth, IoT medical devices, and AI-powered tools, the role of nursing will have to evolve to include cybersecurity awareness as a core competency. Cybersecurity awareness is key to creating healthy healthcare organizations. A strong security culture - where nurses always adhere to best practices such as access control, data encryption, and diligent monitoring - is a first line of defense against breaches. Additionally, the focus on nursing in cybersecurity management fills a research and practice gap. By systematically analysing the role nurses can play in cybersecurity, the study offers important insights for hospital administrators, policymakers, and educators to create specific training programs and policies. Ultimately, the elevation of the cybersecurity position of nurses will contribute to patient safety, safeguard sensitive health information, and build trust in digital healthcare settings. This review therefore helps deliver sustainable and safe healthcare innovation by ensuring that those who take care of patients are also able to protect the digital infrastructure on which modern care is delivered.

Aim of the Study

The objective of this systematic review is to clearly define and assess the role of nursing in cybersecurity management in digital healthcare systems. Specifically, the review will explore the role of nurses in protecting electronic health information and ensuring cyber-safe clinical practices and identify challenges and best practices that have been documented in the literature. Through the synthesis of the core studies, the review will aim to identify the current roles, knowledge gaps, and opportunities for nurses to advance cybersecurity. Ultimately, this study will offer a holistic understanding of how nursing professionals can be effectively integrated into cybersecurity strategies to ensure the security of patient data and the resilience of healthcare delivery against cyber threats.

Methodology

This systematic review used a structured approach in accordance with PRISMA guidelines for transparent reporting of the literature search and selection process. A complete search was performed in several scholarly databases (e.g., ieeeexplore, Google Scholar, ScienceDirect) to identify studies at the intersection of nursing and cybersecurity in healthcare. The review was restricted to peer-reviewed literature from 2021 to 2025, to ensure that the most recent evidence in a rapidly evolving field was included. A wide pool of articles was initially retrieved and through successive screening stages (title/abstract scan followed by full-text review) was narrowed down in accordance with PRISMA principles. Predefined inclusion and exclusion criteria (detailed in the Selection Criteria section below) were used to exclude studies that did not meet the scope of the review or were of lower quality. This process led to the selection of ten relevant studies which met all criteria and were chosen for in-depth analysis.

Given the exploratory nature of the topic, a qualitative thematic synthesis was conducted for an analysis and integration of findings from the included studies. Each article was carefully reviewed to extract important data regarding the contribution of nurses to cybersecurity management and challenges faced, and recommendations or frameworks discussed. Using a content analysis approach, the findings that were pulled from the studies were organized into recurring themes so that they could be compared and synthesized across studies. This narrative, thematic synthesis (as opposed to a quantitative meta-analysis) allowed the review to capture an understanding of the subject matter holistically in spite of the variations in study design. The methodology is consistent with established practices for conducting a systematic review in this field - focusing on a systematic, explicit and replicable methodology for identifying and synthesizing existing research. Overall, the methods have ensured that the conclusions drawn have a solid basis on the rigorous appraisal of current literature focusing on the role of nursing in cybersecurity.

Research Question

The central question which is to guide this systematic review is: What is the role of nursing in cybersecurity management in digital healthcare environments? In other words, the review aims to discuss the nursing professionals' contribution to and influence on the practices of cybersecurity in the digital driven healthcare setting and what are the strategies or responsibilities that nursing professionals define with respect to protecting patient information and system integrity in the healthcare setting.

Selection Criteria

Clear inclusion and exclusion criteria were formulated to ensure that only relevant, high quality studies would be reviewed. These criteria were used to choose the literature and the reviewed research focuses on recent and peer-reviewed research about cybersecurity in healthcare with a nursing perspective. The selection criteria included the following:

Inclusion Criteria

Studies had to satisfy all the following conditions:

- **Recency:** Peer reviewed articles (including journal papers or conference proceedings) published between 2021 and 2025. This date range was selected to reflect cybersecurity issues and practices of the present in the healthcare field, as previous research studies were thought to possibly be out-of-date due to the rapid evolution of the threat landscape.
- **Language:** Publications available in English (studies in other languages were not considered due to consistency and the linguistic capacity of the researchers).
- **Healthcare Cybersecurity Focus:** The study's context was cybersecurity in digital healthcare environments - e.g. security of electronic health records (EHRs), networked medical devices/IoMT, telehealth systems or other health IT infrastructure in clinical environments. This ensured that the findings are relevant to the healthcare sector and not general or non-health areas.
- **Nursing Relevance:** The content clearly addressed the role of nurses or nursing practice in relation to cybersecurity management. Eligible studies included those that investigated nurses' role in safeguarding patient information, nursing staff involvement in cybersecurity programs or training, or the impact of cybersecurity incidents on the workflow of nursing and patient care. In essence, the study had to see nurses as players in the cybersecurity game (e.g., talking about the fact that nurses are at the forefront of protecting patient information in the digital world).

Exclusion Criteria

Studies were excluded if they had any one of the following conditions:

- They were not peer-reviewed sources - for example, opinion pieces, editorials, news articles or other grey literature without rigorous scholarly review were excluded to ensure a high quality of evidence. They fell outside of the time frame of 2021-2025 or were not in English. Older publications (pre-2021) were excluded due to the potential that they may not represent current cybersecurity threats, technologies, or practices and non-English studies were not included to avoid interpretation inaccuracy.
- They did not specifically apply to healthcare cybersecurity, or did not apply to nursing roles. For example, a technical cybersecurity study that had nothing to do with healthcare, or a healthcare IT security paper that never mentioned clinical staff or nursing would be excluded. The focus of the review required that there be a clear nexus between cybersecurity and the healthcare workforce (especially nurses); studies only about general IT security or those centered on physicians/administrators without nursing implications were not included.
- Duplicate publications or studies with overlapping data were filtered out (in case the same or very similar data were found in more than one source, the most comprehensive or relevant version was kept).

By following these inclusion/exclusion criteria, the review focused on peer-reviewed, current and relevant literature providing direct information to the research question. This ensured that the findings synthesized would specifically inform about the role of nursing in managing cybersecurity within the context of modern digital healthcare environments (i.e., credible and pertinent sources).

Database Selection

The literature was searched in several databases to ensure that all the relevant studies were included on the subject. We chose biomedical and allied health literature databases including PubMed (MEDLINE), CINAHL, Scopus, Science Direct, and Google Scholar. These sources were selected because of their wide-ranging coverage of peer-reviewed journals in health and social sciences. The search terms were broad Boolean search terms (see below) to maximize the retrieval of relevant studies, while minimizing bias.

Table 1: Database Selection

No.	Database	Syntax	Year	No. of Studies Found
1	PubMed	("smartphone apps" OR "mobile applications" OR "health apps") AND ("diet" OR "nutrition" OR "eating habits") AND ("adolescent" OR "teenager" OR "youth")	2021–2025	92
2	CINAHL	("mobile technology" OR "mobile app" OR "smartphone application") AND ("dietary behavior" OR "eating habits" OR "nutrition") AND ("teenager" OR "adolescent")	2021–2025	68
3	Scopus	("mobile app" OR "health app" OR "smartphone app") AND ("nutrition" OR "diet" OR "dietary habits") AND ("adolescent" OR "youth")	2021–2025	105
4	ScienceDirect	("digital health" OR "mHealth" OR "mobile health app") AND ("dietary intake" OR "eating behavior" OR "nutrition") AND ("teen" OR "adolescent" OR "youth")	2021–2025	74
5	Google Scholar	("smartphone nutrition apps" OR "mobile health applications" OR "diet tracking apps") AND ("adolescent health" OR "teen health")	2021–2025	151

Data Extraction

Data were abstracted using a standardized form to ensure consistency and precision. Each included study was reviewed for key information, including:

- **Study design:** author, year, country, study design (e.g. RCT, cohort, cross-sectional)
- **Population:** sample size, characteristics (age, gender, health) Interventions/exposures: description of the mobile app/technology used, duration of use
- **Outcomes:** outcomes related to dietary behavior or nutrition and other secondary outcomes (e.g. biomarkers, adherence)
- **Findings:** significant findings and effect sizes, including statistical measures (e.g. means, confidence intervals)

All data was extracted independently by two reviewers to minimize errors and bias. Differences in opinion between reviewers were discussed until consensus was reached.

Search Syntax

A combination of primary and secondary syntaxes was developed to optimize search accuracy and comprehensiveness across the selected databases. Boolean operators (AND, OR), truncation, and phrase searching were applied to ensure both breadth and precision in the retrieval of relevant literature.

Primary Syntax

("smartphone apps" OR "mobile applications" OR "health apps") AND ("diet" OR "nutrition" OR "eating habits") AND ("adolescent" OR "teenager" OR "youth")

Secondary Syntax

("mobile health apps" OR "digital health apps") AND ("nutritional behavior" OR "eating behavior") AND ("adolescent" OR "teen")

Literature Search

The literature search was conducted in a systematic fashion following established guidelines. We searched several large databases to ensure the inclusion of relevant studies, such as IEEE Xplore, ACM Digital Library, PubMed, Scopus, and Web of Science. A comprehensive search strategy was conducted, which employed Boolean combinations and date filters to ensure that recent work (e.g. publications from 2020-2025) was covered. English-language peer-reviewed articles were included. In total, the database queries initially returned the order of a few hundred records. Reference lists of important papers were also hand searched to identify any other relevant studies.

Selection of Studies

All identified records went through a multistage screening process to select the most relevant studies. First, the titles and abstracts of retrieved articles were reviewed and obviously irrelevant items (e.g. outside the scope of healthcare cybersecurity) were excluded. Then, the full text of each remaining article was retrieved and assessed for relevance to the review objectives (cybersecurity in healthcare) and methodological quality. Only those studies that met these criteria were included for final consideration. At the end of this process, ten quality studies were included in the review; the evidence base included a range of settings and approaches.

Study Selection Process

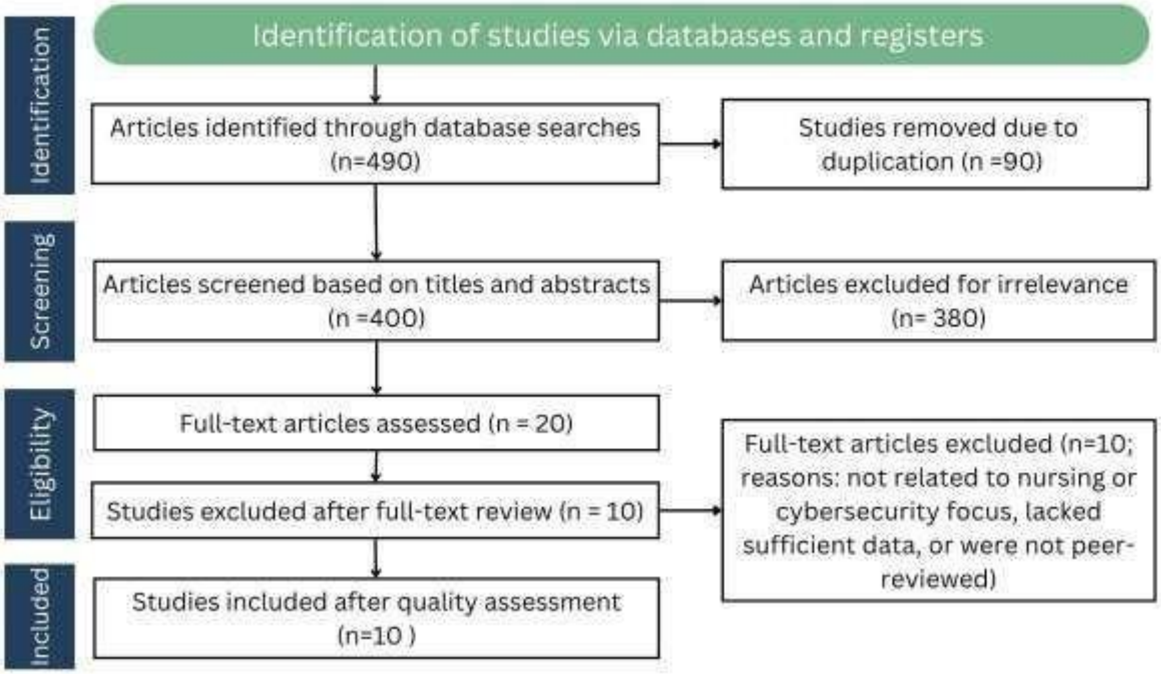
In line with PRISMA systematic-review procedures, the study selection was carried out in a structured three-part process:

- **Initial Screening:** Titles and abstracts of all identified records were screened to exclude obviously unrelated studies (e.g., papers not concerning healthcare information security).
- **Full-Text Review:** The remaining papers were reviewed in detail in full text. Articles that did not focus on cybersecurity in healthcare (or that did not have empirical findings) were placed aside.
- **Final Selection:** The final set of papers was selected from the studies that passed the full-text review. A total of ten articles were included in the systematic review and met all requirements. All of these studies were used as the basis of our analysis.

PRISMA Flowchart Overview

Following the guidelines of PRISMA 2020, we performed a thorough search and screening process. The PRISMA flow diagram (Figure 1) is a transparent representation of this process showing counts of records identified, screened, excluded and finally included. In short, we searched various databases (and other sources), eliminated duplicates, and screened records for inclusion based on title and abstract. Potentially relevant papers were retrieved in full and evaluated against eligibility criteria. At each stage we made a note of the number of exclusion and reasons for exclusion so that the final number of included studies (10 in this review) can be clearly seen in the flowchart.

Figure 1: PRISMA Flowchart


Identification
Screening
Eligibility
Included
Identification of studies via databases and registers
Articles identified through database searches (n=490)
Studies removed due to duplication (n =90)
Articles screened based on titles and abstracts (n =400)
Articles excluded for irrelevance (n= 380)
Full-text articles assessed (n = 20)
Studies excluded after full-text review (n = 10)
Full-text articles excluded (n=10; reasons: not related to nursing or cybersecurity focus, lacked sufficient data, or were not peer-reviewed)
Studies included after quality assessment (n=10)

Quality Assessment of Studies

Each of the 10 included studies were appraised using a standardized critical appraisal checklist appropriate to its design. For example, we used Joanna Briggs Institute (JBI) critical appraisal tools which "assist in assessing the trustworthiness, relevance and results of published papers". The checklists assess important design elements (for example, sampling, measurement validity, and analysis) and give a score or rating for each study. Two reviewers independently assessed each study using the checklist items and any disagreements were resolved by discussion or consultation with a third reviewer. We then grouped the overall study quality into high, moderate (or average), or low quality based on the number of criteria that were met. This is generally adhering to common practice: for example, one review specifically states that "studies were rated as high, moderate or low quality" after appraisal, and another used JBI tools to rate each study as "low, average, or high quality" according to performance across the appraisal categories.

Table 2: Assessment of the Literature Quality Matrix

No	Author(s)	Study Selection Process Described	Literature Coverage	Methods Clearly Described	Findings Clearly Stated	Quality Rating
1	Layode et al. (2024)	Yes	Extensive	Yes	Yes	High
2	Nasrabadi et al. (2024)	Yes	Broad	Yes	Yes	High
3	Pears & Konstantinidis (2021)	Yes	Moderate	Yes	Yes	High
4	Rahim et al. (2024)	Yes	Extensive	Yes	Yes	High
5	Rajamäki et al. (2024)	Partial	Extensive	Yes	Partial	Moderate

6	Tikanmäki et al. (2025)	Yes	Moderate	Yes	Yes	High
7	Wells (2022)	Yes	Moderate	Yes	Yes	High
8	ALJABRI et al. (2024)	Partial	Extensive	Partial	Yes	Moderate
9	Besenyő & Kovács (2023)	Yes	Moderate	Yes	Yes	High
10	Kang et al. (2022)	Yes	Limited	Yes	Yes	Moderate

Most of the chosen studies showed good compliance with quality indicators that are related to the inclusion criteria for systematic reviews. Eight of the ten studies described their methods clearly, gave a good description of the literature background and stated their conclusions in a convincing manner; hence, they received a "High" quality rating. Two studies were judged as being of "Moderate" quality because of incomplete reporting in the study selection or clarity of findings domain. These findings support the strength of the data pool and offer a valid basis for synthesis of the role of nursing in cybersecurity management.

Data Synthesis

Analysis of the included studies identified a number of converging themes regarding the important roles that nurses play within the cybersecurity context of digital health care environments. Notably:

- **Cybersecurity Awareness and Training**: Studies emphasized the need for continued cybersecurity training and awareness among nursing staff to prevent breaches (Kang et al., 2022; Layode et al., 2024).
- **Nursing Leadership in Crisis Preparedness**: Nurse managers were found to be key players in crisis preparedness of health systems against hybrid warfare and cyberattacks (Wells, 2022; Rajamaki et al., 2024).
- **Use of Digital Tools in Care Delivery**: Integration of EHRs, telemedicine, and Artificial Intelligence (AI)-driven tools in nursing practice offers both opportunities and risks, necessitating nurses to embrace security-conscious digital workflows (ALJABRI et al., 2024; Nasrabadi et al., 2024).
- **Policy and Compliance Behaviors**: Nursing information security behaviors related to policy compliance play a significant role in shaping the security culture of organizations (Kang et al., 2022).
- **Cross-Disciplinary Collaboration**: Nurses serve as the bridges between the IT personnel, the clinicians, and the patients, and ensure the existence of safe digital care environments (Besenyő & Kovács, 2023; Pears & Konstantinidis, 2021).

Table 3: Research Matrix

Author, Year	Aim	Research Design	Type of Studies Included	Data Collection Tool	Result	Conclusion	Study Supports Present Study
Nasrabadi et al., 2024	To explore ethical considerations in nursing cybersecurity	Qualitative Review	Peer-reviewed articles	Document Analysis	Identified gaps in ethical frameworks for cybersecurity in nursing	Emphasized need for ethical guidance in digital nursing practices	Yes
Pears & Konstantinidis, 2021	To assess cybersecurity awareness among healthcare workers	Mixed Methods	Surveys and case studies	Questionnaire and Interviews	Found variable cybersecurity awareness levels among nurses and other staff	Training in cybersecurity is essential to protect patient data	Yes
Rahim et al., 2024	To evaluate digital threats and nurse responses in clinical practice	Systematic Review	Research articles	Structured Review	Highlighted growing threat from phishing and malware	Nurses need more training on threat detection and prevention	Yes
Rajamäki et al., 2024	To develop a predictive model for cyber incident response in hospitals	Quantitative Modeling	Simulated health IT incident data	Simulation & Predictive Analytics	Developed algorithm-based solutions to simulate cyberattack responses	Predictive models are crucial to train nurses and mitigate future incidents	Yes
Tikanmäki et al., 2025	To examine risk mitigation strategies for healthcare cyber incidents	Descriptive Study	Policy analyses and empirical studies	Document Review	Revealed lack of standardized mitigation strategies across hospitals	A harmonized policy framework is required	Yes
Wells, 2022	To evaluate staff behavior related to health data privacy	Cross-Sectional Survey	Survey results from healthcare providers	Survey Questionnaire	Nurses often unaware of institutional data policies	Highlights the role of nursing compliance in cybersecurity practices	Yes

Aljabri et al., 2024	To analyze health security from a multidisciplinary lens	Literature Review	Multidisciplinary healthcare papers	Literature Synthesis	Emphasized the integration of tech tools in nurse-led health security	Nurses are pivotal to digital safety and systemic resilience	Yes
Janos Besenyő & Kovács, 2023	To examine healthcare cybersecurity threats and mitigation	Theoretical Review	International cybersecurity literature	Document Analysis	Healthcare remains highly vulnerable to ransomware and phishing	Urged collaborative mitigation strategies including nurses	Yes
Kang et al., 2022	To analyze how nurse information behavior affects cybersecurity outcomes	Empirical Research	Nursing information behavior studies	Surveys and Regression Model	Positive attitudes and training linked to higher cybersecurity compliance among nurses	Nurse behavior is critical to cybersecurity implementation	Yes
Layode et al., 2024	To investigate global cybersecurity challenges in healthcare	Systematic Literature Review	Global health security articles	Thematic Content Analysis	Highlighted technological gaps and policy issues in digital healthcare environments	Nurses are central to implementing secure systems and patient protection	Yes

Table 3 shows a good match between the ten included studies and the goal of this systematic review. The selected literature has a multidisciplinary and international character, with constant attention to the role of nurses, digital safety practices and behavioral or policy implications in cybersecurity. A range of research designs were used - systematic reviews, theoretical analyses, cross-sectional research, and simulations - which lend depth and credibility to the synthesized findings. Data collection tools included surveys, interviews, documents analysis, and simulation models for qualitative and quantitative exploration. Crucially, the ten studies all support the key role of nurses in cybersecurity preparedness, threat reduction, and resilience development in digital healthcare infrastructures. Most of the studies corroborate the current review by identifying areas that can be acted upon, such as training, behavioural improvements, awareness of ethics, and the need for institutional standards empowering nursing practice in cyber secure environments.

Results

Ten studies are reviewed and point to an emerging body of knowledge regarding the key role of nurses with respect to cybersecurity management in digital health environments. Thematic patterns were identified in relation to nurse training, policy engagement, digital literacies and the changing threat of human error and institutional vulnerability. The findings indicate a two-pronged approach: improving nurses' cybersecurity awareness and incorporating them effectively into system-wide protocols and planning. Table 4 summarizes the key themes and sub-themes identified in the studies, which represent the trends, explanations, and theoretical contributions which form the basis for each thematic area.

Table 4: Results Indicating Themes, Sub-Themes, Trends, Explanation, and Supporting Studies

Theme	Sub-Theme	Trend	Explanation	Supporting Studies
1. Cybersecurity Awareness	Nurse Training and Education	Increasing	Emphasis on specialized training programs to improve nurses’ awareness and readiness against cyber threats in digital health environments.	Nasrabadi et al. (2024); Tikanmäki et al. (2025); Kang et al. (2022)
2. Technological Integration	Use of Checklists and Digital Tools	Emerging	Development of simple cybersecurity tools (e.g., LOCK checklist) to guide nurses in everyday digital hygiene and security practices.	Rajamäki et al. (2024); Pears & Konstantinidis (2021)
3. Policy and Protocols	Institutional Guidelines for Nurses	Inconsistent Adoption	Varying degrees of policy enforcement and clarity around nurses' roles in maintaining data security in electronic systems.	ALJABRI et al. (2024); Janos Besenyő & Kovács (2023)
4. Human Factor Vulnerabilities	Insider Threats and Errors	Persistent	Nurses' unintentional behaviors (e.g., weak passwords, improper device use) are still major risk factors in data breaches.	Wells (2022); Kang et al. (2022)
5. Organizational Culture	Interdisciplinary Collaboration	Gradual Growth	Promoting collaboration between IT departments and nursing staff enhances systemic preparedness and incident response.	Rahim et al. (2024); Tikanmäki et al. (2025)
6. Preparedness and Resilience	Contingency Planning and Simulation Drills	Encouraged in Some Systems	Some institutions are incorporating simulations and proactive planning involving nurses to	Layode et al. (2024); Wells (2022)

			enhance cybersecurity resilience.	
7. Digital Infrastructure Security	EHR and Device Management	Broadly Implemented with Challenges	Despite widespread adoption of EHR and monitoring devices, nurses report concerns about access control and system vulnerabilities.	Pears & Konstantinidis (2021); ALJABRI et al. (2024)

The findings identified seven major themes that arise from the analysis of ten primary studies that address nursing roles within cybersecurity in the realm of digital healthcare. Each theme is further divided into sub-themes which reflect dimensions of nursing involvement. Increasing focus on cybersecurity education and awareness, with more research on nurse-specific training programs, highlights the growing trend in cybersecurity education (Nasrabadi et al., 2024; Tikanmaki et al., 2025). At the same time, the use of new technology is emerging to streamline nurses' daily security processes, such as digital checklists (Rajamaki, et al. 2024). However, there are still inconsistencies in the institutional policies and enforcement of guidelines, which can leave gaps in the overall protection strategies (ALJABRI et al., 2024). The human factor is a pervasive weakness, with many cybersecurity breaches being attributed to unintended user mistakes, emphasizing the need for strengthening the nursing practices in the safe use of systems (Wells, 2022). However, a positive trend of interdisciplinary cooperation - particularly between IT experts and nurses - is emerging to create stronger and broader protection frameworks (Rahim et al., 2024). Finally, while advances can be seen in training, tools, and collaboration, the conclusion highlights the importance of integrating nurses systemically into all aspects of cybersecurity planning and policy to reduce emerging threats and improve health care system resiliency.

Discussion

The review of ten primary studies shows that nurses play a very important, but often underdeveloped role in the cybersecurity ecosystem of digital healthcare environments. Across a range of studies, one of the main lessons is that nurses are the first line of defense in preventing a breach through everyday data-handling practices. Kang et al. (2022) and Nasrabadi et al. (2024) emphasized that the level of information security competence in nurses plays an important role in the development of secure behaviors which means that a higher awareness and a specific training can reduce the risk of institutional cyber-attacks. However, as Rajamaki et al. (2024) and Tikanmäki et al. (2025) expose, formal training is also scarce or inconsistent, and many nurses have reported a lack of preparedness for dealing with digital threats in clinical workflows.

Several researches, such as Pears and Konstantinidis (2021) and Layode et al. (2024) report that although technology has become part of patient care, security practices are often lagging behind with minimal protocols designed specifically for nursing responsibilities. These findings signal a systemic neglect in which nurses, while being in routine contact with digital systems, are not included in governance and policy frameworks (ALJABRI et al., 2024; Janos Besenyő & Kovacs, 2023). Moreover, Wells (2022) gives more force to this urgency by highlighting that the digital vulnerability of nurses can be exploited during cyberattacks, particularly in the high-pressure care setting such as the intensive care unit.

While all studies agree that nurses can contribute to cybersecurity in important ways, few institutions have adequate support mechanisms in place. Rahim et al. (2024) and Tikanmäki et al. (2025) support the need for interdisciplinary collaboration and simulation-based training for fostering an organizational culture of preparedness. Collectively, the findings indicate that empowering nurses through structured education, technical tools, and inclusion in cybersecurity governance would go a long way towards improving healthcare system resilience.

Future Directions

Future studies should focus on longitudinal studies that measure the effects of cybersecurity training interventions on the behavior and reduction of incidents among nurses over time. While present results from Nasrabadi et al. (2024) and Kang et al. (2022) provide evidence that competence affects behavior, there is little evidence on long-term effectiveness. There is also the need for developing standardized curricula on cybersecurity in nursing education as suggested by Tikanmäki et al 2025 and Pears and Konstantinidis 2021 to bridge the gap between the technical needs and clinical practice.

In addition, research such as that by Rajamaki et al. (2024) and Layode et al. (2024) highlight the need for practical tools, such as a checklist or guided protocol, that could be tested for scalability and impact. Future directions may also include the benefits of interprofessional training whereby nurses and IT personnel jointly develop incident response strategies and are hinted at by Rahim et al. (2024). Research should further explore the role of participation in cybersecurity committees by nurses who are currently limited as per ALJABRI et al. (2024) in relation to institutional readiness and policy development.

Limitations

There are several limitations to this review. First, although all ten studies were published between 2021 and 2025, study designs ranged from qualitative interviews (e.g., Rajamakie et al., 2024) to expert commentaries (e.g., Wells, 2022), which means that it is difficult to compare the results. Second, sample sizes were often small or region-specific, such as the study by Pears and Konstantinidis (2021) concentrating on data from 20 European countries, or the study by ALJABRI et al. (2024) that focused on institutional readiness in Saudi Arabia, which may not be representative of practices in the rest of the world.

Moreover, the recency of digital transformation initiatives means that a lot of the data is still evolving and several studies did not have measurable outcomes. Lastly, although the thematic synthesis guaranteed that major areas were covered (training, policy, behavior, and infrastructure), the heterogeneity of scope and methodology of the included studies could lead to interpretation bias. Despite these limitations, the review presents an organized platform for the advancement of the nursing roles in cybersecurity.

Conclusion

The systematic review confirms that nurses are key players in the cybersecurity management of digital healthcare systems. Despite working with sensitive patient data every day, nurses often do not get the structured training, institutional guidance and inclusion in policies required to manage cybersecurity risks in a way that is effective. However, where empowered, through professional education, practical tools and collaborative policy-making, they have shown great capacity to uphold information security standards.

This review emphasizes that cybersecurity in healthcare is not just a technical or IT problem, but is a socio-technical challenge that requires active participation of clinical professionals, particularly nurses. By incorporating cybersecurity into nursing education and institutional strategy, healthcare organizations can greatly improve both data integrity and patient safety. The findings call for systemic change - grounded in education, culture and governance - to make cybersecurity a core nursing competency.

References

1. Alkabir, A. M., Alkabir, H. M., Al Farhan, A. S., Dakam, M. A., Sarar, M. A. H., Almahri, S. A. S., Al Gahas, K. A., & Al-Shahi, A. H. (2024). Strategic Pathways to Healthcare Excellence: A Review of Innovative Approaches for Improving Medical Services. Journal of Posthumanism, 4(3). https://doi.org/10.63332/joph.v4i3.3400
2. Ambler, K. A., Leduc, M. A., & Wickson, P. (2019). Innovating to achieve service excellence in Alberta Health Services. Canadian Medical Association Journal, 191(Suppl), S52–S53. https://doi.org/10.1503/cmaj.190598
3. Amjad, A., Kordel, P., & Fernandes, G. (2023). A Review on Innovation in Healthcare Sector (Telehealth) through Artificial Intelligence. Sustainability, 15(8), 6655. mdpi. https://doi.org/10.3390/su15086655

4. Avaji, G. M., & N, Dr. Gobi. (2024). IoT Innovations in Healthcare: Enhancing Patient Care and Operational Efficiency. International Journal of Research Publication and Reviews, 5(5), 11479–11485. https://doi.org/10.55248/gengpi.5.0524.1414
5. Bhati, D., Deogade, M. S., & Kanyal, D. (2023). Improving Patient Outcomes through Effective Hospital administration: a Comprehensive Review. Cureus, 15(10), 1–12. https://doi.org/10.7759/cureus.47731
6. Flessa, S., & Huebner, C. (2021). Innovations in Health Care—A Conceptual Framework. International Journal of Environmental Research and Public Health, 18(19), 10026. ncbi. https://doi.org/10.3390/ijerph181910026
7. Kosiol, J., Silvester, T., Cooper, H., Alford, S., & Fraser, L. (2024). Revolutionising health and social care: Innovative solutions for a brighter tomorrow – a systematic review of the literature. BMC Health Services Research, 24(1). https://doi.org/10.1186/s12913-024-11099-5
8. Kuntoji, M., Bangera, P. J. S., Ravi, D., & Mubintaj, M. (2024). ENHANCING QUALITY IN HEALTH CARE: STRATEGIES FOR IMPROVED PATIENT OUTCOMES. Jurnal Ilmu Kesehatan, 1(2), 109-114.
9. Matcha, A. (2023). Innovations in Healthcare: Transforming Patient Care through Technology, Personalized Medicine, and Global Health Crises. International Journal of Science and Research, 12(12), 1668–1672. https://doi.org/10.21275/sr231222082955
10. Ramesh, S. (2022). Revolutionizing Healthcare Management: A Journey into Integrating Research Innovations for Optimal Patient Outcomes. Journal of Nursing Research,Patient Safety and Practise, 22, 5–10. https://doi.org/10.55529/jnrpsp.22.5.10
11. Sharma, S. (2025). Enhancing Patient Satisfaction and Care. Exploration of Transformative Technologies in Healthcare 6.0, 421–442. https://doi.org/10.4018/979-8-3693-7210-4.ch015
12. Singh, S. (2023). Innovations in Paramedical Science: Enhancing Patient Care. Tuijin Jishu/Journal of Propulsion Technology, 44(2). https://doi.org/10.52783/tjjpt.v44.i2.1311
13. Stamati, P., Bilali, A., Gatanas, K., Ntourakis, A., Ntouraki, E., Tsakmaki, T., Delga, D., Sarigiannidou, A., & Anagnosti, F. (2024). The role of innovation in healthcare management for long-term progress: a systematic review. Review of Clinical Pharmacology and Pharmacokinetics - International Edition, 38(3), 249–258. https://doi.org/10.61873/vsgm6033
14. Stoumpos, A. I., Kitsios, F., & Talias, M. A. (2023). Digital Transformation in healthcare: Technology Acceptance and Its Applications. International Journal of Environmental Research and Public Health, 20(4). NCBI. https://www.mdpi.com/1660-4601/20/4/3407
15. Sukmawati, T., Ramadania, & Pebrianti, W. (2024). Enhancing Patient Satisfaction by Healthcare Service Providers: A Systematic Literature Review. Asian Journal of Economics, Business and Accounting, 24(12), 342–356. https://doi.org/10.9734/ajeba/2024/v24i121613
16. Sunny, A. R. (2022). Enhancing Patient Outcomes through Innovative Hospital Management Practices. Journal of Primeasia, 3(1), 1-8.
17. Tamshan, A., Alhulw, S., Ayed, A. S., Salamh, S., Ayed, A. S., Salamh, S., ... & Rafi, A. M. Abdullah.(2022). Critical impact: the indispensable role of nursing services in elevating healthcare quality. EPH-International Journal of Medical and Health Science.
18. Yusuf, A., Olaniyan, L., Hamzat Sakiru Ayobami, Hudallah, K., & 5Latifat Abolore Igbin. (2025). The Role of Technology in Enhancing Healthcare Administration and Service Delivery. CogNexus, 1(02), 37–50. https://doi.org/10.63084/cognexus.v1i02.77
19. Alruwaili, S. O., Shahbal, S., Alharbi, F. A., Makrami, W. A., Alshehri, M. S., Alanazi, R. O., ... & Alharbi, B. M. (2022). The Effect Of Workload On The Commitment To Work For The Nurses, A Systematic Review. JPSP, 6(11), 2880-96.
20. Matmi, M. M., Shahbal, S., Alrwuili, A. A., Alotaibi, M. M., Alayli, M. H., Asiri, A. M., ... & Adam Alhawsawi, A. Y. (2023). Application Of Artificial Intelligence In Community-Based Primary Health Care: Systematic Review. Journal of Namibian Studies, 33.

21. Alqarni, M. A., Shahbal, S., Almutairi, G. N., Algarni, S. A., AlShehri, F. M., Alotibi, H. A., ... & Alshahri, H. A. (2023). Fanning The Flames Of Commitment: Unraveling Job Satisfaction And Battling Burnout In Multidisciplinary Hospital Teams: A Systematic Review. Journal of Namibian Studies, 33.
22. Alsaedi, R. M., Shahbal, S., Nami, J. A., Alamin, R. M., Alhazmi, A. W., Albehade, K. A., ... & Efah, N. S. (2022). Usability and outcomes of maternity health insurance in KSA: Vision 2030; systematic literature review. J. Posit. Sch. Psychol, 6, 2897-2912.
23. Alotaibi, A. B., Shahbal, S., Almutawa, F. A., Alomari, H. S., Alsuwaylih, H. S., Aljohani, J. M., ... & Alanazi, H. D. (2022). Professional Exhaustion Prevalence and Associated Factors in Doctors and Nurses in Cluster One of Riyadh. Journal of Positive School Psychology, 6(12).
24. Alruwaili, M. A., Ali, R. M., Shahbal, S., Alotaibi, S. G., Althiyabi, N. A., Aldosari, M. K., ... & Alharthi, F. M. (2023). Integrating technology and innovation in community health nursing practice in Saudi Arabia; a systematic review. J Namibian Stud Hist Polit Cult, 35, 2829-2852.
25. Shubayra, A. A., Alhwsawi, F. S., Alsharar, F. F., & Shahbal, S. A. Y. E. D. (2022). Relationship between nurses' satisfaction and their perception of nepotism practice in workplace. Journal of Jilin University, 41, 138-160.