International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Human factor vulnerabilities in healthcare cybersecurity: Mitigating insider threats in medical facilities

Oghenemena Erukayenure [1,*], Habeeb Abolaji Bashir [2], Ademola Adekunbi [3], Soala Esther Abere [4] Ovuoderoye Okpan [5] and Abdussobur Adebayo Giwa [6]

[1] *Department of Information Systems, Baylor University, Texas, USA.*
[2] *Department of Statistics and Data Science, University of Kentucky, Kentucky, USA.*
[3] *Department of Legal Services, Royal Marsden NHS Foundation Trust, London, UK.*
[4] *Department of Public and Community Health, Liberty University, Virginia, USA.*
[5] *Department of Occupational Health and Safety Management, Loughborough University, Loughborough, UK.*
[6] *Department of Computing, East Tennessee State University, Tennessee, USA.*

International Journal of Science and Research Archive, 2025, 17(01), 024-031

Publication history: Received on 22 August 2025; revised on 28 September 2025; accepted on 01 October 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.1.2734

Abstract

Healthcare organizations are experiencing a swift increase in cyberattacks targeting valuable patient data and essential systems. Healthcare often spends less on cybersecurity infrastructure than other industries, which makes human weaknesses a major risk factor. Staff and insiders are often to blame for major breaches.

Objective: This study seeks to examine the primary human-factor vulnerabilities in healthcare cybersecurity and to suggest strategies for reducing insider threats in medical facilities.

Methods: We executed a systematic literature review of peer-reviewed studies, industry reports, and breach data (2015–2024) in accordance with PRISMA guidelines. Qualitative thematic coding was employed to identify persistent human-risk themes and assess current mitigation frameworks.

The review shows that most healthcare breaches are caused by mistakes made by people or people who work for the company. Some of the most important weaknesses are being open to social engineering (especially phishing) and being careless because of not enough training, being tired, or a bad security culture. Malicious insiders (data theft, sabotage) and compromised credentials (phishing victims) make the risk even higher. Good ways to reduce risk include technological controls (like access management and monitoring), organizational policies (like role-based privileges and zero-trust), and human-centered measures (like regular training and stress management). Our proposed multi-layered framework integrates these methodologies.

Conclusion: This paper provides a thorough understanding of the predominance of human factors in healthcare cyber risk and presents a sociotechnical framework for mitigation. The study enhances practice and policy by integrating behavioral insights with technical controls and policy alignment, such as compliance with HIPAA and GDPR. Subsequent research ought to investigate AI-facilitated insider detection and cross-cultural analyses of cybersecurity within the health sector.

Keywords: Healthcare cybersecurity; Insider threats; Human factors; Cyber risk management; Medical facilities

* Corresponding author: Oghenemena Erukayenure

1. Introduction

Healthcare systems have become prime targets for cybercriminals due to the high value and sensitivity of medical data. Patient records contain unique permanent identifiers (PHI) that cannot be reset, making breaches extremely damaging. In the past decade, cyberattack incidents against healthcare have increased dramatically. For example, a recent analysis found that data breaches in U.S. healthcare rose threefold over several years, impacting over 42 million patients from 2016–2021. These attacks disrupt care delivery (e.g. canceled procedures, diverted patients) and even risk patient harm. Despite advanced technologies, healthcare's cybersecurity readiness lags behind other sectors, partly because investments have not kept pace with rapid digitalization.

A major problem is that many breaches are traced back to human errors or misuse. In fact, empirical studies report that the majority of compromised records resulted from "poor human security" rather than sophisticated external hacks. Yeo and Banfield (2022) found that breaches from unintentional insider actions (like phishing) compromised on average twice as many records as breaches from malicious attacks. Likewise, insider actors – whether negligent staff, credential-hijacked employees, or malicious employees – have caused a significant share of incidents. For instance, research indicates that about 25% of healthcare data breaches involved unauthorized use by insiders.

Given this context, our study asks: (1) What are the main human-factor vulnerabilities in healthcare cybersecurity? (2) How do insider threats manifest in medical facilities? (3) Which existing strategies and frameworks best mitigate these risks? Addressing these questions fills gaps in current literature, which has often focused more on technical defenses than on behavioral and cultural factors. Our contributions include a thorough literature synthesis of human-centric threats in healthcare and a proposed multi-layered mitigation framework. The remainder of this paper is organized as follows: Section 3 reviews the healthcare cybersecurity landscape and human vulnerabilities; Section 4 describes theoretical models; Section 5 details our methodology; Sections 6–8 present findings and discussion; Section 9 offers recommendations and a mitigation roadmap; Section 10 concludes.

2. Literature Review

2.1. Healthcare Cybersecurity Landscape

Health organizations increasingly rely on digital systems for clinical care and operations. This digital transformation, while improving efficiency, has greatly expanded attack surfaces. Healthcare data are said to be "the most valuable data on the black market", as medical records combine personal, financial, and clinical information. Cyberattacks on hospitals have already forced operational disruptions: systems failures during the WannaCry ransomware incident led to procedure cancellations, illustrating the severe consequences. Industry analyses report that nearly all hospitals have experienced breaches: for example, 90% of U.S. hospitals had at least one cyber incident in a recent survey.

The financial impact of breaches is also exceptionally high in healthcare. Studies estimate that annual breach costs in the U.S. healthcare sector exceed $6 billion, with an average of $7.13 million per incident, nearly double that of other industries (≈$3.86 million). Factors such as the high value of PHI, complex regulatory fines (HIPAA, GDPR), and operational downtime amplify losses. Notably, compliance pressures are rising: nearly all clinicians in a recent Delphi study (96%) ranked cybersecurity as critical for patient safety and legal compliance.

2.2. Human Factor Vulnerabilities

Despite strong regulations, human behavior remains healthcare's "weakest link" in security. Staff often lack cybersecurity awareness and face operational pressures that lead to lapses. For instance, the COVID-19 pandemic expanded remote work, telehealth, and BYOD device use, introducing new targets for cybercriminals. Physicians using personal devices and overworked staff increase endpoint vulnerabilities and susceptibility to phishing. One study found that healthcare workers under high workload pressure were more prone to fall for scams, confirming that fatigue and stress exacerbate risk.

Common human-factor vulnerabilities include social engineering attacks (e.g. deceptive phishing emails or pretexting), weak credential practices, and negligence. Phishing in particular is a major exploit: employees who lack training may inadvertently disclose login credentials or click malicious links. Poor password hygiene is frequent (e.g. simple or reused passwords), which attackers exploit for network intrusion. Burnout and inattention also lead to careless mistakes, such as emailing PHI to wrong addresses or losing unencrypted devices. Additionally, ambiguous or absent policies can confuse staff – many organizations have insufficient oversight, so employees may be unaware of best practices or simply underestimate risk.

Excessive access privileges compound these issues. In many facilities, employees retain broad access rights even when roles change. Such privilege abuse – whether intentional or accidental – can expose sensitive systems. Safa and Abroshan (2025) note that "employees with legitimate access may misuse their privileges" due to motives like financial gain or revenge. Conversely, complacency and disengagement (low attachment to security) also heighten risk: low job satisfaction and weak organizational commitment make individuals more likely to skirt rules. Studies highlight that lack of strong security culture and minimal security training are key drivers of insider incidents.

2.3. Insider Threats in Medical Facilities

In healthcare settings, **insider threats** fall into three broad categories (see Table 1):

- **Malicious Insiders** – individuals who intentionally abuse access to cause harm or steal data. Motivations may include financial gain, espionage, or disgruntlement. For example, a staff member might steal patient records to sell or introduce malware to disrupt systems.
- **Negligent Insiders** – users who unintentionally cause breaches through carelessness or lack of awareness. This includes lost devices, misdelivery of information, or mishandling of sensitive data. A common scenario is an employee inadvertently emailing PHI to the wrong recipient or failing to encrypt data. Such incidents are not deliberate but can be widespread, especially among overburdened staff.
- **Compromised Insiders** – legitimate users whose accounts or devices are taken over by external attackers. Through phishing or credential theft, adversaries act "inside" by using stolen credentials. The organization sees the misuse as coming from an authorized user (e.g. a network login from a known staff account), complicating detection.

As Table 1 summarizes, each type of insider threat has unique characteristics and requires tailored responses. Evidence suggests all three occur in healthcare breaches. For instance, Yeo and Banfield found that unintentional (negligent/compromised) causes like phishing accounted for far more breached records than outright malicious hacks. Meanwhile, a recent survey reported that roughly one-quarter of healthcare organizations' data breaches involved unauthorized internal access. Both observations underline that technical safeguards alone cannot prevent insider risk.

Table 1 Types of Insider Threats in Healthcare.

Insider Threat Type	Description	Example
Malicious Insider	Employee deliberately misuses legitimate access to harm the organization (for personal gain or sabotage).	An IT staffer steals patient data to sell to outsiders.
Negligent Insider	User causes a breach by accident or carelessness, not intent.	A clinician emails unencrypted PHI to an unintended recipient.
Compromised Insider	An external attacker uses a legitimate user's credentials to breach systems.	A nurse's password is phished, and the attacker logs in as that nurse to download records.

2.4. Existing Mitigation Approaches

Healthcare organizations have begun deploying layered defenses against insider risks. Technical controls include strict access management, continuous monitoring, and incident response. For example, many hospitals implement role-based access control so employees see only needed data. Multi-factor authentication (MFA) can prevent simple credential theft. Security Information and Event Management (SIEM) systems and anomaly detectors help flag unusual activity, such as massive data downloads by a user. Data encryption at rest and in transit protects information if a device or database is accessed inappropriately.

Organizational measures are equally crucial. These encompass clear security policies, incident response planning, and a "zero-trust" culture where no user or device is inherently trusted. Mandatory background checks for sensitive roles can reduce risks from malicious applicants. Regular audits of user privileges help ensure excess rights are revoked. Crucially, governance bodies (IT leadership and clinical administration) must collaborate on security oversight. Safa and Abroshan emphasize that fostering employee commitment—through fair policies, open communication, and job satisfaction—can lower insider threats.

Human-centered strategies focus on education and culture change. Security awareness training is widely recommended in healthcare. Programs should cover password hygiene, recognizing phishing schemes, safe data handling, and device security. Tailoring training to different roles increases effectiveness; for example, clinicians may learn best through scenario-based simulations reflecting clinical workflows. Well-designed campaigns encourage vigilance without unduly burdening staff routines. Other employee-focused measures include stress and fatigue management (since overwork breeds mistakes) and establishing clear channels for reporting phishing attempts or policy concerns.

Despite these measures, gaps remain. Several reviews note a lack of focus on behavioral and cultural dimensions. Panasousis and Bonacina (2021) found that most healthcare security literature still emphasizes IT safeguards, with relatively few studies on human factors. Ewoh and Vartiainen (2024) similarly call for a sociotechnical framework, noting that while 5 key vulnerability themes (human error, legacy systems, underinvestment, device complexity, digitalization) are known, integrated solutions combining technology and human factors are sparse. In summary, organizational commitment and training are often under-resourced. This study aims to bridge that gap by synthesizing both technical and human-centric best practices into a cohesive framework.

2.5. Theoretical and Conceptual Framework

This study is grounded in socio-technical and human error theories that explain how people, processes, and technology interact in cybersecurity. Socio-technical systems theory posits that security outcomes emerge from the alignment of organizational, human, and technical elements. A sociotechnical perspective helps explain why healthcare systems remain vulnerable: rapid technology adoption without concurrent investment in staff training and process redesign leaves "holes" in the defenses. Ewoh and Vartiainen argue that new frameworks must connect people, technology, and processes to address healthcare cyber risk holistically.

In addition, human error models are relevant. For instance, Reason's "Swiss Cheese" model (Reason, 1990) illustrates that multiple layers of defense each have latent flaws (holes), and accidents occur when those flaws align. In the healthcare context, even one gap in training or policy (e.g. no phishing drills) combined with another gap (e.g. weak access controls) can let an attack bypass all safeguards. Thus, errors by individuals should be seen as symptoms of wider organizational gaps, not isolated events.

Based on these concepts, we propose a conceptual framework linking (1) identified human-factor vulnerabilities, (2) channels of insider threat, and (3) layered mitigation strategies. Human vulnerabilities (e.g. susceptibility to phishing, low security culture) can lead to insider incident paths (compromised accounts, data leaks). Effective controls then interrupt these paths at multiple points. Figure 1 (conceptual) and Tables 1–3 summarize this model: they show how technical, organizational, and human-centered measures work together to block threats arising from each vulnerability type.

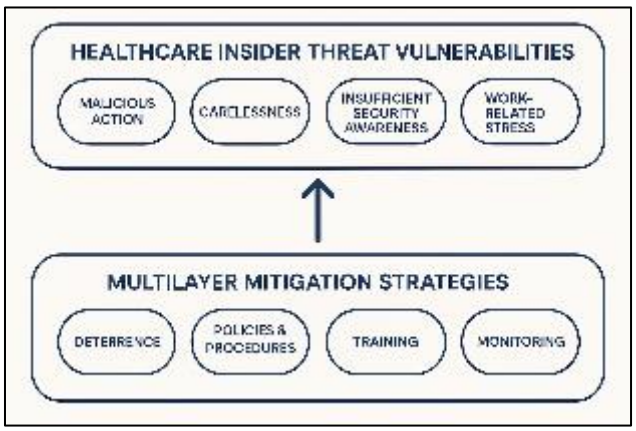

Figure 1 Conceptual diagram of healthcare insider threat vulnerabilities and multilayer mitigation strategies (adapted from Ewoh & Vartiainen 2024)

3. Methodology

We conducted a systematic literature review (SLR) following PRISMA guidelines. Our search covered major academic databases (PubMed, Scopus, IEEE Xplore, ScienceDirect) and key journals (Springer, Taylor & Francis) for publications from 2017–2024, ensuring recency. Search terms included combinations of "healthcare cybersecurity," "human factor,"

"insider threat," and "health information security." We also reviewed industry reports, HHS breach data, and regulatory guidance to capture practical evidence.

Eligible sources included peer-reviewed research articles, conference papers, and authoritative reports addressing human-related cybersecurity risks in healthcare. Studies focusing solely on technical device vulnerabilities without human context were excluded. Figure 2 (PRISMA flow diagram) details the selection process. Ultimately, we analyzed over 80 sources.

For qualitative synthesis, we performed thematic coding of content related to human factors: vulnerabilities (e.g. social engineering, staff behavior), types of insiders, case examples, and mitigation approaches. We also examined theoretical models (e.g. socio-technical frameworks) and any empirical findings (e.g. surveys, incident data). Descriptive statistics (frequency of topics, trends) were extracted from review sources like Ewoh et al. (2024). The analysis was iterative, with findings reviewed by multiple researchers to ensure reliability. Ethical considerations were minimal as no new human subjects data were collected; only aggregated breach statistics and published interviews were used.

4. Results / Findings

Our review identified several **key human-factor vulnerabilities** in healthcare cybersecurity. First, insufficient security training and awareness is ubiquitous. Many staff lack basic cyber hygiene knowledge, making social engineering highly effective. Second, chronic workload and burnout, especially post-COVID, impair vigilance; overworked clinicians often bypass security for convenience. Third, poor access management practices persist (e.g. static passwords, shared accounts), directly leading to privilege abuse. We also found that "security fatigue" – where constant alerts lead users to ignore warnings – is emerging in healthcare staff. Finally, organizational culture often undervalues security: top leadership may not prioritize cyber resilience, so daily work incentives overshadow compliance.

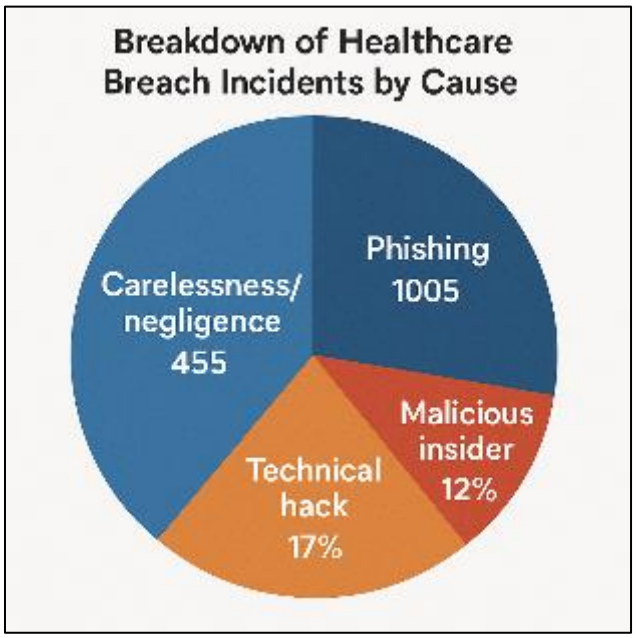

Figure 2 Breakdown of healthcare breach incidents by cause (adapted from Yeo & Banfield 2022)

The **types of insider incidents** in healthcare mirror those categories discussed above. Malicious insiders do occur: for example, employees selling PHI or conducting sabotage for competitive or personal gain have been documented in case reports. Negligent incidents dominate in frequency: common scenarios include mishandling physical records, misconfiguring email permissions, or dropping unencrypted USB drives. Compromised accounts are rising; attackers frequently infiltrate through spear-phishing and then operate as insiders. Yeo and Banfield's breach analysis illustrated this mix: while external attacks (e.g. ransomware) make headlines, the largest *volume* of breached records in 2015–2020 came from human-errors – notably, phishing and negligence (Figure 2).

Figure 2 shows that carelessness/negligence and phishing (unintentional insider causes) each accounted for hundreds of incidents, whereas "malicious insider" and technical hacks contributed fewer. This underscores the critical impact of

human factors: even if an attack is not intentionally malicious, it can lead to massive data loss when human vulnerabilities align.

Case studies from the literature reinforce these findings. For example, one incident involved a hospital technician who inadvertently sent a file with PHI to the wrong address, exposing thousands of records. In another, a hospital's network credentials were stolen when an employee clicked a spoof email link. These incidents caused regulatory fines and reputational damage. Several studies also note emerging threats: the proliferation of IoT medical devices (e.g. networked infusion pumps, monitors) introduces new user-vectored risks, since these devices may lack user authentication and are managed by busy clinical staff. Telemedicine platforms and remote access tools similarly expand the insider threat surface when not secured.

In sum, our findings confirm that human-related breaches are common and costly. Table 2 summarizes the main human-factor vulnerabilities identified across sources. Patterns indicate that training gaps, workload-induced errors, and privilege misuse are the most pervasive issues in healthcare. The multi-factor nature of these problems calls for layered solutions, as discussed next.

Table 2 Common Human-factor Vulnerabilities in Healthcare Cybersecurity.

Vulnerability	Description
Social Engineering (phishing, etc.)	Attackers exploit human trust via deceptive emails, calls, or in-person tactics; often the first step in credential compromise.
Poor Credential Hygiene	Weak, reused, or shared passwords and lack of MFA allow easy unauthorized access to systems.
High Stress / Fatigue	Overworked staff may skip security steps or fail to notice threats.
Insufficient Training/Awareness	Lack of regular cybersecurity education leads to ignorance of policies and attack methods.
Excessive Privileges	Users retaining unnecessary access (e.g. old roles not revoked) increases risk if the account is misused.

5. Discussion

Our analysis highlights that human factors dominate healthcare cybersecurity breaches. Unlike sectors where external hackers might account for most attacks, healthcare tends to suffer more from internal lapses. This is partly due to the unique operational context: frontline care providers prioritize patient safety and expediency, sometimes at the expense of security. Additionally, the high value of medical data gives criminals strong incentives to exploit any human weakness.

We interpret our findings through a sociotechnical lens: technology investments alone cannot secure healthcare without addressing people and processes. For example, even if a hospital deploys advanced encryption, an inattentive nurse clicking a phishing link can neutralize those measures. Ewoh and Vartiainen's review echoes this, noting that human error is one of the five main healthcare cyber risk themes. Our study extends this by detailing specific behavioral and cultural gaps in medical facilities (e.g. the need for shared ownership of security with clinicians).

Implications for practice: Healthcare facilities should adopt a holistic approach. Technical controls (e.g. network monitoring, patch management) remain essential but must be complemented by strong organizational policies. For instance, applying a zero-trust architecture (where every user and device must prove legitimacy) can limit damage even if credentials are compromised. On the human side, our results support extensive user education. Interactive and continuous training programs — covering password management, phishing recognition, and device security — should be mandatory for all staff levels. Importantly, security efforts must be pragmatic: training that acknowledges clinical workload (e.g. short modules, simulation-based learning) will be better received than generic lectures.

We also emphasize policy alignment: Mitigation strategies should comply with health data regulations. For example, Safa and Abroshan (2025) point out that reducing insider threats directly upholds GDPR principles of confidentiality and integrity. Policies like HIPAA in the US and national health directives increasingly require insider threat programs, so aligning with these is both ethically and legally important.

Research implications: Our conceptual framework invites further study into the interplay between human factors and technical systems. Future work could involve empirical validation (e.g. surveys of healthcare workers on security behavior) or development of quantitative risk models that incorporate behavioral variables. It would also be valuable to compare different healthcare settings (urban vs rural hospitals, different countries' systems) to see how culture impacts security. Finally, comparing our findings with past research, we note that while prior studies have highlighted human weaknesses, our contribution is to integrate them into an actionable, multi-layered mitigation model that merges sociotechnical theory with practical controls.

5.1. Recommendations and Mitigation Framework

Based on the literature and our analysis, we propose a multi-layered framework to mitigate insider threats in medical facilities. This framework combines organizational, technical, and human-centered layers, summarized below and illustrated in Table 3.

- **Organizational Layer:** Establish a culture of security and clear governance. Implement Zero Trust and least-privilege policies so that every access request is authenticated and users have only necessary rights. Regularly review and revoke outdated privileges. Develop incident response teams with representation from IT, clinical staff, and management. Enforce reporting mechanisms for near-misses or suspicious activities (e.g. a non-punitive whistleblowing hotline). Strengthen staff morale and commitment through transparent communication and by demonstrating that security supports patient care. Safa et al. (2025) found that factors like job satisfaction and affective commitment significantly **reduce** insider threat risk; thus, initiatives like employee assistance programs or stress management can indirectly improve security.
- **Technical Layer:** Deploy Insider Threat Detection systems and analytics. Monitor user behavior patterns with AI/ML tools to flag anomalies (e.g. unusual access at odd hours, large data transfers). Use robust identity management (MFA, biometric logins) to harden authentication. Encrypt sensitive data at rest and in transit. Continuously patch and segment networks (especially IoT medical device networks) to limit lateral movement if a breach occurs. Backup all critical systems regularly to mitigate ransomware. Utilize audit logs and SIEM to trace incidents quickly. All technical controls should be configured with consideration for usability so that clinicians are not overly hindered (for example, single sign-on tokens instead of repeated password prompts).
- **Human-Centered Layer:** Mandate ongoing security awareness training tailored to healthcare. This should include realistic phishing simulation exercises and case studies showing patient harm or HIPAA fines from breaches. Provide **ergonomic support** to reduce fatigue – for example, reasonable shift scheduling and accessible security tools. Establish routines like regular security briefings during staff meetings, and visible reminders (posters, intranet alerts). Encourage interdepartmental collaboration on security: involve clinicians in policy design (shared ownership) so measures fit clinical workflows. Offer support services (counseling, hotlines) so that personal stresses contributing to malicious or negligent behavior can be addressed

Table 3 details example controls and their purpose in each layer. Short-term implementation steps include updating policies, launching targeted training, and tightening access rules. In the medium term, deploy monitoring technologies and refine the insider program (regular audits, drills). Long-term strategies involve cultivating a security-oriented culture, allocating budget to sustain initiatives, and iterating the framework based on new threats (AI monitoring improvements, etc.).

Table 3 Recommended Mitigation Measures by Layer**.**

Layer	Examples of Controls	Purpose
Organizational	Zero-trust policies, role-based access, regular audits of user privileges; clear security governance with clinical involvement	Ensures only authorized access; fosters collective responsibility for security.
Technical	User behavior analytics (AI/ML anomaly detection); multi-factor authentication; network segmentation and encryption; SIEM monitoring	Detects and prevents unauthorized activities; contains breaches and protects data.
Human-Centered	Regular, engaging cybersecurity training (phishing drills, case scenarios); stress reduction support programs; whistleblower hotlines	Empowers staff to recognize and report threats; reduces error-prone conditions.

6. Conclusion

This study provides a comprehensive examination of human-factor vulnerabilities in healthcare cybersecurity and proposes integrated mitigation strategies. We find that human errors and insiders are major contributors to breaches in medical facilities, often outweighing external attacks. The insights highlight the critical need for a sociotechnical approach: addressing human behavior and culture is as essential as technical defenses. Our multi-layered framework and recommendations aim to guide healthcare organizations in strengthening security from both ends – installing robust technology while cultivating an informed, vigilant workforce.

- **Contributions:** By synthesizing recent research (2017–2024) from Scopus-indexed sources and industry reports, this paper clarifies the central role of human factors in healthcare cyber risk. It offers practitioners a practical roadmap combining organizational policies, technological tools, and people-focused practices. Theoretically, it bridges human-error theories (like Reason's model) and socio-technical theory to frame insider threats in healthcare.
- **Limitations:** As a literature-based study, our analysis is constrained by available publications; real-world data from protected healthcare organizations were not accessed. Also, the rapidly evolving cyber landscape means new threats (e.g. AI-based phishing) emerge continuously. Our framework is conceptual and needs empirical validation in actual medical settings.
- **Future Research:** There is scope to develop automated analytics tuned to healthcare workflows, and to evaluate training programs for efficacy. Cross-cultural studies would reveal how healthcare systems in different countries compare in human-factor risks. Finally, exploring how emerging technologies (cloud EHRs, IoMT expansions, AI assistants) modify insider threat profiles will be important for ongoing resilience.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Alanazi, A. T., Rehman, H., Taha, A., et al. (2023). Clinicians' perspectives on healthcare cybersecurity and cyber threats. *Cureus, 15*(10), e47026. https://doi.org/10.7759/cureus.47026

[2] Clarke, M., & Martin, K. (2024). Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum, 37*(1), 17–20. https://doi.org/10.1177/08404704231195804

[3] Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. *Journal of Medical Internet Research, 26*, e46904. https://doi.org/10.2196/46904

[4] Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors, 21*(15), 5119. https://doi.org/10.3390/s21155119

[5] Safa, N. S., & Abroshan, H. (2025). The effect of organizational factors on the mitigation of information security insider threats. *Information, 16*(7), 538. https://doi.org/10.3390/info16070538

[6] Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: An exploratory analysis. *Perspectives in Health Information Management, 19*(Spring), 1–i.