Cybersecurity challenges in healthcare: mitigating risks in a rapidly evolving digital landscape

Arina Alexei[1], Ion Bolun[1], Anatolie Alexei[2]
[1]Department of Software Engineering and Automatics, Technical University of Moldova, Chisinau, Republic of Moldova
[2]Department of Telecommunications and Electronic Systems, Technical University of Moldova, Chisinau, Republic of Moldova

Article Info

Article history:

Received Dec 10, 2024
Revised Jun 20, 2025
Accepted Sep 27, 2025

Keywords:

Cybersecurity
Digital transformation
Healthcare
Patient safety
Risk management

ABSTRACT

The rapid digital transformation of the healthcare sector brings significant benefits but also exposes institutions to escalating cybersecurity risks. This study analyzes vulnerabilities such as ransomware, supply chain compromises, and insider threats, drawing on international reports from World Health Organization (WHO), Healthcare Information and Management Systems Society (HIMSS), Ponemon, and Verizon. The paper contributes a unique mitigation framework that consolidates three strategic pillars: i) continuous cybersecurity training for medical staff, ii) deployment of advanced technological safeguards, and iii) establishment of collaborative incident reporting mechanisms. Beyond mapping current threats, the study provides policy-oriented guidance for strengthening resilience in both developed and emerging healthcare systems. With healthcare breaches costing an average of $10.1 million per incident, the findings highlight the urgent need for coordinated action to ensure patient safety, service continuity, and institutional trust.

Corresponding Author:

Arina Alexei
Department of Software Engineering and Automatics, Technical University of Moldova
168 Stefan cel Mare si Sfant Blvd., Chisinau 2004, Republic of Moldova
Email: arina.alexei@tse.utm.md

1. INTRODUCTION

The transition from an industry-based economy to a knowledge-based economy has fundamentally reshaped the role of technology, shifting investments toward digital tools, research, and human capital. In healthcare, digitalization has become both necessary and unavoidable [1], driven by factors such as population aging, shortages of physicians, the strain of the COVID-19 pandemic, and the increasing demand for remote medical services. Electronic health records (EHRs), telemedicine, big data, and artificial intelligence/machine learning (AI/ML) applications exemplify how digital healthcare improves efficiency, accessibility, and quality of care.

However, these advancements also introduce growing cybersecurity risks. Healthcare institutions process highly sensitive medical data, and their dependence on interconnected technologies—including internet of medical things (IoMT) devices, AI-driven diagnostics, and robotic systems—expands the attack surface. Recent studies confirm that cybersecurity threats in healthcare are increasing exponentially, with data privacy, patient safety, and service continuity at stake [2], [3]. Addressing these challenges requires a systematic understanding of both technological vulnerabilities and human factors.

This study contributes to filling that gap by analyzing international reports to identify critical threats and by proposing a structured mitigation framework. The novelty of this research lies in consolidating global evidence into three integrated pillars: continuous staff training, advanced technological safeguards, and collaborative incident reporting. By bridging human, technical, and policy perspectives, the paper offers practical guidance for strengthening resilience and ensuring trust in digital healthcare systems.

2. BACKGROUND

In the provision of online services information and communication technology (ICT) plays a central role, by directly contributing to the improvement of medical services, ensuring the access of all citizens to medical services, reducing operational, and administrative costs in medical institutions and enabling the introduction of new models of care delivery, such as telemedicine (Figure 1 illustrates the integration of ICT in healthcare).

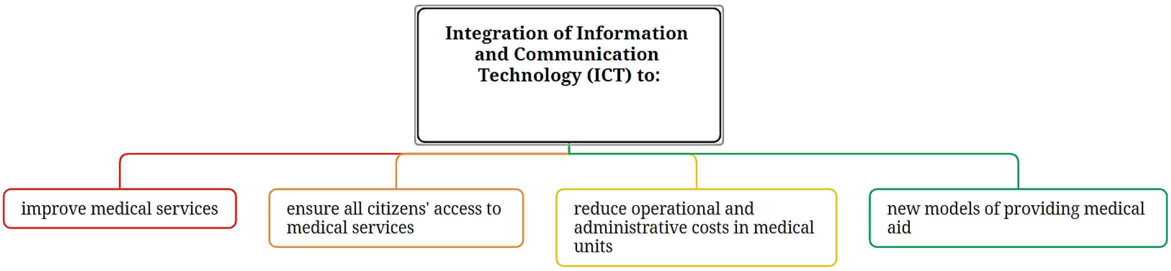

Integration of Information and Communication Technology (ICT) to:
improve medical services
ensure all citizens' access to medical services
reduce operational and administrative costs in medical units
new models of providing medical aid

Figure 1. Integration of ICT in healthcare

As a result, ICT in healthcare has led to the emergence of two widely used concepts: digital healthcare (e-healthcare) and smart healthcare (s-healthcare).

2.1. Digital healthcare

Digital healthcare (e-health) refers to the use of internet-based and information systems to enhance the efficiency, quality, and accessibility of medical services [4], and supporting person-centered care [5]. Its main components include EHRs, telemedicine, health information systems (HIS), mobile health (mHealth), and wearable devices (Figure 2).

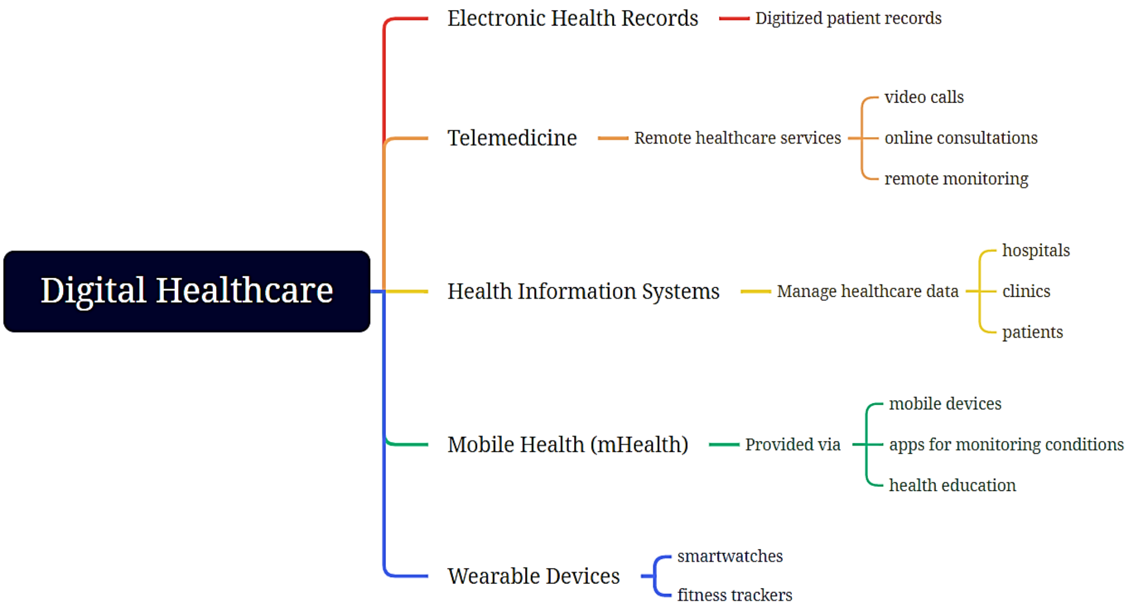


Figure 2. Digital healthcare components

EHRs enable secure, real-time access to clinical data and improve care coordination [5], [6]. Telemedicine addresses accessibility barriers for elderly, rural, or chronically ill populations, and proved essential during the COVID-19 pandemic [5], [7]. mHealth complements telemedicine by supporting continuous monitoring and self-management, aggregating data from applications and mobile devices [8], [9]. Recent research emphasizes that modern wearable devices play a pivotal role in remote patient monitoring systems, providing continuous health data acquisition and enabling early detection of anomalies. However, their integration into healthcare infrastructures also raises challenges related to interoperability, energy efficiency, and the secure transmission of sensitive patient information [10]. Modern wearables integrate sensors for vital signs and synchronize with smartphones and computers, with emerging potential for early disease prevention and clinical decision support [11], [12].

Overall, digital healthcare supports data-driven care, optimizes processes, and reduces operational costs, providing the foundation for safe and scalable remote health services.

2.2. Smart healthcare

Smart healthcare builds upon digital healthcare by integrating advanced technologies—IoMT, AI/ML and deep learning, big data and data mining, and cloud–fog–edge computing—to provide personalized, real-time services (Figure 3).

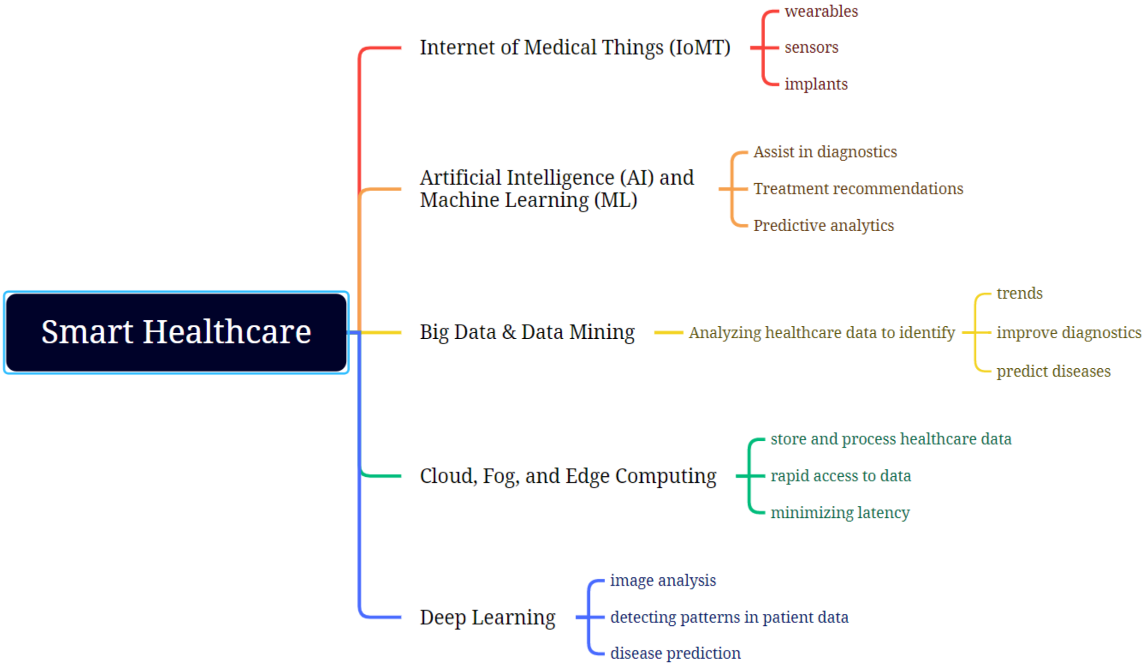

Smart Healthcare
Internet of Medical Things (IoMT)
wearables
sensors
implants
Artificial Intelligence (AI) and Machine Learning (ML)
Assist in diagnostics
Treatment recommendations
Predictive analytics
Big Data & Data Mining
Analyzing healthcare data to identify
trends
improve diagnostics
predict diseases
Cloud, Fog, and Edge Computing
store and process healthcare data
rapid access to data
minimizing latency
Deep Learning
image analysis
detecting patterns in patient data
disease prediction

Figure 3. Smart healthcare components

IoMT connects wearable, sensor-based, and implantable devices within clinical platforms for monitoring and diagnostics, already widely adopted in telemedicine and smart hospitals [13]. AI/ML support prevention and early detection, enhance data analysis, and enable precision medicine [14], [15], while big data/data mining offer large-scale analytics [16]. Cloud computing underpins digital infrastructures, with fog/edge technologies reducing latency for time-sensitive scenarios [17].

The core objective of smart healthcare is proactivity: improving clinical outcomes, reducing errors, and increasing system efficiency (Figure 3), while setting the stage for robust cybersecurity strategies discussed in the following sections.

2.3. Cyber security risks in healthcare

The digital transformation of healthcare, while essential, significantly expands the cybersecurity threat surface. Interconnected systems, outdated infrastructure, and highly sensitive medical data create vulnerabilities to service interruptions, data theft, and system manipulation. The key domains of cybersecurity risks are illustrated in Figure 4, highlighting the complex interplay of technological, organizational, and human factors.

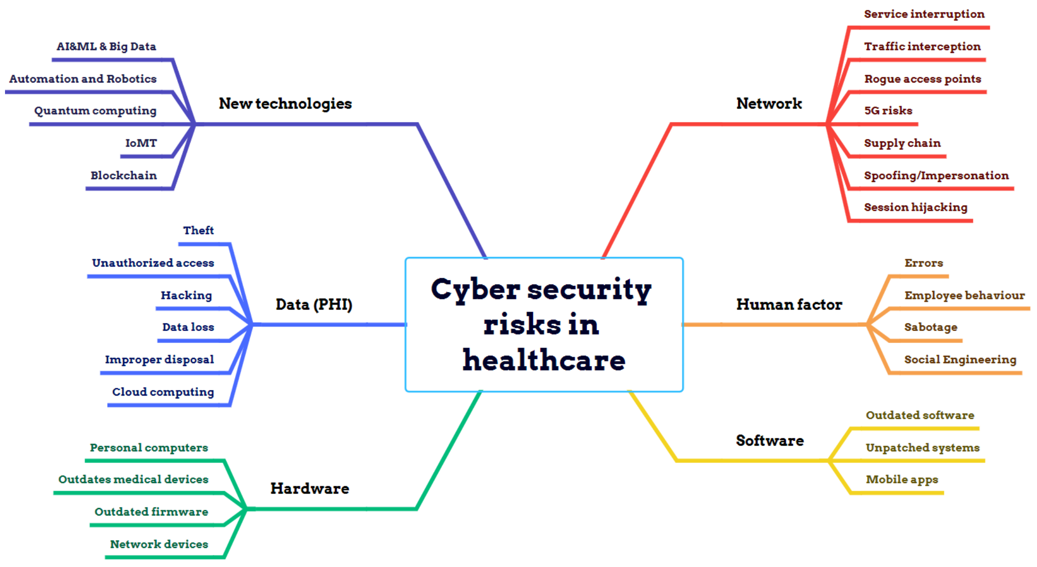


Figure 4. Cyber security risks

Healthcare networks are vulnerable to various types of cyberattacks, including service interruptions, traffic interception, spoofing, and session hijacking. While the adoption of 5G technology offers faster data transmission, it also increases the complexity of securing network infrastructures, thereby amplifying cybersecurity risks. Disruptions to network services can have immediate and serious consequences, such as the interruption of patient access to care, cancellation of appointments, and even the shutdown of medical departments due to the inaccessibility of essential devices.

Healthcare personnel remain a central vulnerability, often due to human error or manipulation through social engineering techniques, such as phishing. Insider threats, whether resulting from deliberate sabotage or unintentional actions—can also lead to substantial data breaches and operational failures.

Many healthcare institutions continue to rely on outdated or unpatched software systems, making them easy targets for cybercriminals. Additionally, the use of unsecured mobile applications further compounds the issue, as attackers can exploit app vulnerabilities or gain unauthorized access through stolen devices that lack robust authentication mechanisms.

Recent incidents highlight the severity of these risks. In 2024, a large-scale ransomware attack disrupted digital services across 100 hospitals in Romania, severely affecting patient care. Attackers exploited outdated systems and unpatched vulnerabilities to encrypt critical medical records, demanding a ransom of 3.5 BTC (approximately 157,000 EUR). The incident caused delays in procedures and interruptions in emergency services due to the compromise of HIS software, with the initial breach traced back to the primary software vendor. Also, in 2024, another major security breach occurred in France, where approximately half of the country's population—around 33 million individuals—had their medical records compromised. The attackers used a phishing campaign targeting healthcare employees to gain access to sensitive data, including medical histories. This event underscored the lack of cybersecurity awareness and the inadequacy of email filtering systems in healthcare institutions.

In 2023, a large-scale cyberattack targeted Ukraine's leading telecommunications provider, which supports hospital and emergency service connectivity. Ransomware was deployed to encrypt patient records and disable medical devices, effectively halting critical operations. This attack formed part of a broader offensive on Ukraine's digital infrastructure, significantly affecting the healthcare sector.

Multiple studies have shown that the global medical field has historically been underfunded in terms of information technology (IT) infrastructure and cybersecurity investments [2], [18]. This has led to the continued use of outdated equipment, often lacking necessary software updates and security patches. Such vulnerabilities significantly increase the risk of cyberattacks, thereby endangering patient safety.

Protected health information (PHI) is a critical asset in healthcare and a frequent target for cybercriminals. Threats such as data theft, hacking, and improper disposal of sensitive information are widespread. Patient records typically contain extensive personal and medical data, which are considerably more sensitive than financial information. With such data, attackers can illegally obtain controlled substances or financial benefits. Consequently, a complete set of medical records can sell for over $1,000 on the dark web [2]. The adoption of cloud computing introduces additional challenges, particularly in securing sensitive data stored in decentralized environments. Ensuring the confidentiality, integrity, and availability of data in the cloud remains a major concern for healthcare providers.

Healthcare systems also rely heavily on devices associated with the IoMT, which present significant security risks. These devices are widely used in intensive care and encompass a range of technologies—from ventilators and infusion pumps to patient monitors, implantable devices, and organ support systems. Cyberattacks targeting these critical devices may not only disrupt services but could also result in fatal outcomes for patients.

Data generated by IoMT devices is highly vulnerable to a range of attacks classified into three main categories [19]: device-level, network-level, and data-level threats. Device attacks, such as side-channel or firmware tampering, exploit both hardware and software weaknesses [20]. Network threats include distributed denial of service (DDoS), man in the middle (MITM), and ransomware [21], while data-specific attacks—like spoofing, exfiltration, or tampering—target the integrity and confidentiality of medical information [22]. Despite existing safeguards such as encryption, access control, and intrusion detection system (IDS), IoMT security remains challenging due to the need for lightweight solutions suited to energy-constrained environments.

The potential consequences of compromised AI-driven systems—such as surgical robots or clinical decision-support tools—can be severe, potentially resulting in misdiagnoses, incorrect treatment recommendations, or procedural errors that jeopardize patient safety.

Although AI and ML technologies form the foundation of smart healthcare systems, they pose significant security concerns related to data privacy, result accuracy, and trust in automated decisions [23]. For instance, the interpretability of ML models, which are often trained on patient data from specific socio-cultural environments, may lead to inaccurate outcomes when applied to diverse populations. Furthermore, AI systems can be targeted by cyberattacks, potentially compromising the integrity of both patient data and clinical recommendations. Numerous studies [24], [25] have demonstrated that AI and ML models, particularly convolutional neural networks (CNNs), are susceptible to adversarial attacks. Techniques such as the fast gradient sign method (FGSM) can intentionally manipulate input data to mislead the model, causing incorrect classifications and undermining the reliability of AI-driven healthcare decisions.

Low levels of digitalization, as in Moldova (20% adoption), also create risks by limiting real-time data access, with severe consequences during crises such as COVID-19 [26].

2.4. Healthcare-specific cyber security threat analysis

To ensure an objective analysis, recent reports published by internationally recognized organizations were reviewed. These include the Healthcare Information and Management Systems Society (HIMSS), the Ponemon Institute—a leading authority in cybersecurity research—the World Health Organization (WHO), and Verizon, a global entity that annually assesses the state of cybersecurity across various industries.

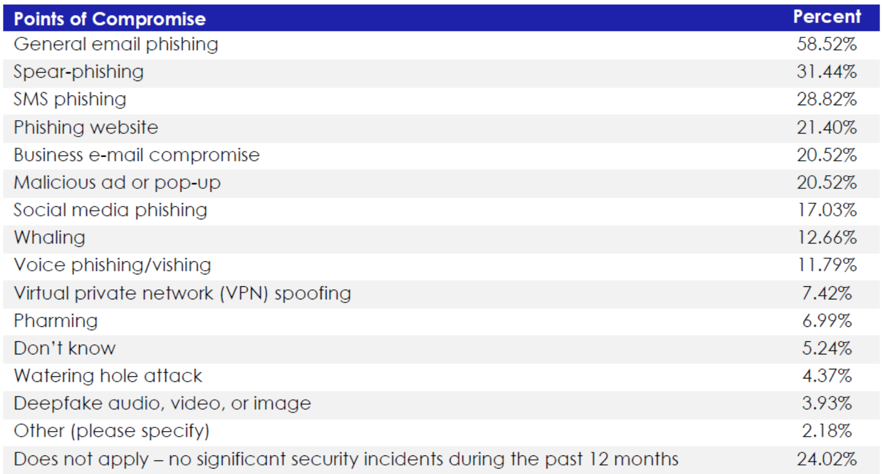
According to the 2024 WHO report titled "Examining the threat of cyber-attack on health care during the COVID-19 pandemic" [27], ransomware remains one of the most serious risks for the healthcare sector. Beyond financial extortion, attackers gain additional value from selling stolen medical records. The main initial vectors of compromise include social-engineering techniques such as phishing and spear phishing, exploitation of the microsoft remote desktop protocol (RDP), and insider threats associated with employee-owned devices, removable media, or unregulated messaging applications.

The report also highlights a rising frequency and scale of malware attacks, driven by two key factors: the designation of healthcare as critical national infrastructure and the persistent underreporting of cybersecurity incidents by medical institutions. This underreporting both reduces sector-wide awareness and increases the attractiveness of healthcare targets to cybercriminals.

These risks are further reinforced by the growth of ransomware-as-a-service (RaaS), also noted in the 2023 HIMSS healthcare cybersecurity survey [28]. According to HIMSS, which gathered responses from 229 cybersecurity professionals across medical organizations worldwide, the most common initial points of compromise in 2023 were phishing, spear phishing, and SMS phishing attacks.

Adding to this concern, recent advances in large language models (LLMs) enable attackers to generate highly convincing phishing messages—grammatically accurate, sentiment-aware, and multilingual—which makes them increasingly difficult for users to detect and filter. A summary of the most common attack vectors targeting the healthcare sector is illustrated in Figure 5.

Ransomware continues to be the most prevalent and disruptive cybersecurity threat to healthcare, with variants such as LockBit and BlackSuit frequently reported; the latter is especially concerning due to the lack of publicly available technical descriptors [28]. Another significant concern is the healthcare supply chain, where the compromise of a single software vendor can trigger cascading effects across multiple dependent institutions. In parallel, the adoption of generative artificial intelligence (GenAI) tools by healthcare staff creates new risks, including unauthorized data leakage, breaches of patient confidentiality, and theft of intellectual property. Moreover, the emergence of quantum computing poses a long-term existential threat to current cryptographic algorithms, endangering the confidentiality of sensitive data both at rest and in transit.



Points of Compromise	Percent
General email phishing	58.52%
Spear-phishing	31.44%
SMS phishing	28.82%
Phishing website	21.40%
Business e-mail compromise	20.52%
Malicious ad or pop-up	20.52%
Social media phishing	17.03%
Whaling	12.66%
Voice phishing/vishing	11.79%
Virtual private network (VPN) spoofing	7.42%
Pharming	6.99%
Don't know	5.24%
Watering hole attack	4.37%
Deepfake audio, video, or image	3.93%
Other (please specify)	2.18%
Does not apply – no significant security incidents during the past 12 months	24.02%

Figure 5. Common attack vectors [28]

Further insights are offered by the Ponemon Institute's 2023 report "Cyber insecurity in healthcare" [29], based on input from 653 cybersecurity professionals worldwide. Ponemon's findings align with WHO and HIMSS, identifying cloud compromise (63%), supply chain attacks (64%), and medical device insecurity (53%) among the most common threats. On average, healthcare organizations experienced 3.7 ransomware incidents over the past two years, with 40% admitting to ransom payments. The consequences were severe: ransomware disrupted medical care in 68% of cases, increased patient mortality by 28%, delayed procedures and tests in 59%, and contributed to complications in 44%. Similarly, corporate email compromise led to operational disruptions in nearly 70% of cases, often delaying testing and lengthening hospital stays.

The 2024 Verizon Data Breach Investigations Report [30] added another critical dimension: insider threats. According to the report, 70% of breaches in healthcare involved internal actors, with financial gain cited as the motive in 98% of cases. Human error (e.g., misdelivery of documents and accidental data loss), abuse of system privileges, and unauthorized intrusions were identified as the most common forms of insider-related compromise. Ransomware remains particularly dangerous in this context because it can block access to systems critical for patient care, potentially leading to life-threatening consequences.

Overall, these reports converge on a clear conclusion: healthcare cybersecurity is undermined by a combination of human factors, outdated infrastructures, and vulnerable supply chains, while the rapid adoption of emerging technologies adds further complexity. These insights form the basis for the results and discussion section, where targeted mitigation strategies are proposed.

3. RESULTS AND DISCUSSION

The findings presented in this article emphasize the significant cybersecurity risks facing the healthcare sector as a result of rapid digitization and increasingly complex infrastructures. The analysis of recent reports from WHO, HIMSS, the Ponemon Institute, and Verizon has revealed critical vulnerabilities that, if not adequately addressed, may lead to severe disruptions in healthcare services and compromise patient safety [27]–[30]. These insights underscore the need to move from threat identification toward concrete mitigation strategies, as outlined below.

Among the most pressing concerns is the limited cybersecurity awareness among end-users. The human factor remains the weakest link in the security chain, with susceptibility to phishing and other social engineering tactics consistently identified as the most common entry point for cyberattacks [27], [28]. This highlights the urgent need for comprehensive cybersecurity education and training for healthcare personnel. Structured initiatives aimed at improving digital hygiene, recognizing manipulation techniques, and adopting secure online practices are essential to strengthening resilience.

Ransomware continues to be the most damaging threat, with variants such as LockBit and BlackSuit capable of severely disrupting medical operations and incurring major financial costs [28], [29]. The cascading effects of supply chain attacks further amplify this risk, as a single compromised vendor can affect multiple dependent institutions. Strengthening supply chain security through recognized standards and rigorous vendor oversight is therefore critical [29].

Emerging technologies also introduce additional vulnerabilities. While AI, IoMT, and cloud computing bring transformative benefits to healthcare, they simultaneously expand the attack surface [16], [21]. AI can be misused for generating highly convincing phishing content [28], IoMT devices are exposed to device-, network-, and data-level attacks [19]–[22], and cloud environments remain frequent targets for account compromise [29]. The looming cryptographic challenges posed by quantum computing further reinforce the need for adaptable cybersecurity frameworks [28].

The Verizon 2024 Data Breach Investigations Report emphasized the growing prevalence of insider threats, with 70% of incidents involving internal actors, most motivated by financial gain [30]. Human error, abuse of system privileges, and unauthorized access remain among the most frequent causes. In parallel, the Ponemon Institute (2023) reported that healthcare organizations experienced an average of 3.7 ransomware incidents over the past two years, with 40% admitting to ransom payments. Consequences included disrupted care in 68% of cases, increased patient mortality by 28%, and delayed procedures in nearly 60% [29]. Similarly, corporate email compromise led to operational disruptions in 69% of cases, demonstrating the profound clinical impact of cyber incidents.

According to IBM (2023), the healthcare sector continues to face the highest global average cost per data breach—estimated at $10.1 million [29]. Beyond financial losses, these incidents delay essential medical procedures, increase complication rates, and in some cases contribute directly to elevated mortality rates. This underlines the urgent need for resilience planning and disaster recovery mechanisms that ensure service continuity during cyber crises.

In particular, for countries where healthcare digitalization is still emerging, the following key recommendations should be prioritized:

- Cybersecurity training: implement structured and continuous education programs tailored for healthcare professionals to reduce human error and increase awareness [27], [28];
- Technological safeguards: deploy advanced solutions such as AI-driven threat detection, endpoint protection, and strong encryption to secure devices and sensitive data [21], [29];
- Collaborative incident reporting: establish mechanisms for reporting and sharing cybersecurity incidents with public authorities or sectoral platforms to improve collective defense [28];
- Regulatory and policy updates*:* strengthen data protection legislation and align with frameworks such as GDPR, HIPAA, and ISO/IEC 27001, adapting them to local healthcare contexts [28], [29].

Additional measures derived from case studies include:

- Regular updates and patch management, complemented by penetration testing to identify vulnerabilities before exploitation;
- Secure data backups and robust disaster recovery plans to minimize downtime during incidents;
- Ongoing social engineering awareness training, supported by automated detection of phishing attempts;
- Implementation of multi-factor authentication (MFA) and role-based access control for stronger identity management;
- Strict policies for the use of smart medical devices and handling of sensitive data;
- Reinforced supply chain security through international standards, best practices, and third-party audits [29], [30].

Taken together, these recommendations highlight the urgent need for a multi-layered, collaborative cybersecurity strategy that integrates human, technological, and policy measures [27]–[30].

4. CONCLUSION

This study shows that mitigating cybersecurity risks in healthcare requires a structured framework built on three pillars: continuous staff training, deployment of advanced security technologies, and collaborative incident reporting. The unique contribution lies in consolidating global threat evidence into a practical mitigation approach that links human, technological, and policy measures. Reinforced by the fact that healthcare breaches cost an average of $10.1 million per incident, the findings underline the urgent need for coordinated strategies that ensure patient safety, service continuity, and trust in digital healthcare systems.

FUNDING INFORMATION

This research was supported by the Technical University of Moldova within the project DACISLab: Virtual Laboratory on Open Data and Open Science in the New Generation of Continuum Computing Systems.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Arina Alexei	✓	✓				✓	✓		✓	✓	✓		✓	
Ion Bolun		✓		✓		✓		✓		✓	✓	✓		
Anatol Alexei	✓			✓		✓	✓	✓	✓	✓	✓		✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis

I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting

Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] A. Garcia-Perez, J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro, and A. Chinnaswamy, “Resilience in healthcare systems: Cyber security and digital transformation,” *Technovation*, vol. 121, pp. 1–11, Mar. 2023, doi: 10.1016/j.technovation.2022.102583.

[2] A. J. Cartwright, “The elephant in the room: cybersecurity in healthcare,” *Journal of Clinical Monitoring and Computing*, vol. 37, no. 5, pp. 1123–1132, Oct. 2023, doi: 10.1007/s10877-023-01013-5.

[3] C. M. Okafor *et al.*, “Mitigating Cybersecurity Risks in the US Healthcare Sector,” *International Journal of Research and Scientific Innovation (IJRSI)*, vol. 10, no. 9, pp. 177–193, 2023, doi: 10.51244/IJRSI.2023.10918.

[4] M. H. da Fonseca, F. Kovaleski, C. T. Picinin, B. Pedroso, and P. Rubbo, “E-health practices and technologies: A systematic review from 2014 to 2019,” *Healthcare (Switzerland)*, vol. 9, no. 9, pp. 1–32, Sep. 2021, doi: 10.3390/healthcare9091192.

[5] T. H. Tebeje and J. Klein, “Applications of e-Health to Support Person-Centered Health Care at the Time of COVID-19 Pandemic,” *Telemedicine and e-Health*, vol. 27, no. 2, pp. 150–158, Feb. 2021, doi: 10.1089/tmj.2020.0201.

[6] L. Coventry and D. Branley, “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,” *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/j.maturitas.2018.04.008.

[7] A. Haleem, M. Javaid, R. P. Singh, and R. Suman, “Telemedicine for healthcare: Capabilities, features, barriers, and applications,” *Sensors International*, vol. 2, pp. 1–12, 2021, doi: 10.1016/j.sintl.2021.100117.

[8] K. Fan and Y. Zhao, ” Mobile health technology: a novel tool in chronic disease management,” *Intelligent Medicine*, vol. 2, no. 1, pp. 41–47, Feb. 2022, doi: 10.1016/J.IMED.2021.06.003.

[9] B. M. C. Silva, J. J. P. C. Rodrigues, I. de la T. Díez, M. López-Coronado, and K. Saleem, “Mobile-health: A review of current state in 2015,” *Journal of Biomedical Informatics*, vol. 56, pp. 265–272, Aug. 2015, doi: 10.1016/j.jbi.2015.06.003.

[10] T. Sivani and S. Mishra, “Wearable Devices: Evolution and Usage in Remote Patient Monitoring System,” in *Studies in Computational Intelligence*, vol. 1021, pp. 311–332, 2022, doi: 10.1007/978-3-030-97929-4_14.

[11] T. Luczak, R. Burch, E. Lewis, H. Chander, and J. Ball, “State-of-the-art review of athletic wearable technology: What 113 strength and conditioning coaches and athletic trainers from the USA said about technology in sports,” *International Journal of Sports Science and Coaching*, vol. 15, no. 1, pp. 26–40, Feb. 2020, doi: 10.1177/1747954119885244.

[12] J. Lutz, D. Memmert, D. Raabe, R. Dornberger, and L. Donath, “Wearables for integrative performance and tactic analyses: Opportunities, challenges, and future directions,” *International Journal of Environmental Research and Public Health*, vol. 17, no. 1, pp. 1–26, Dec. 2020, doi: 10.3390/ijerph17010059.

[13] C. Huang, J. Wang, S. Wang, and Y. Zhang, “Internet of medical things: A systematic review,” *Neurocomputing*, vol. 557, pp. 1–18, Nov. 2023, doi: 10.1016/j.neucom.2023.126719.

[14] Z. Ahmed, K. Mohamed, S. Zeeshan, and X. Q. Dong, “Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine,” *Database*, pp. 1–35, Jan. 2020, doi: 10.1093/database/baaa010.

[15] W. DeGroat, V. Venkat, W. Pierre-Louis, H. Abdelhalim, and Z. Ahmed, “Hygieia: AI/ML pipeline integrating healthcare and genomics data to investigate genes associated with targeted disorders and predict disease,” *Software Impacts*, vol. 16, pp. 1–4, May 2023, doi: 10.1016/j.simpa.2023.100493.

[16] L. B. Furstenau *et al.*, “Big data in healthcare: Conceptual network structure, key challenges and opportunities,” *Digital Communications and Networks*, vol. 9, no. 4, pp. 856–868, Aug. 2023, doi: 10.1016/j.dcan.2023.03.005.

[17] Q. V. Khanh, N. V. Hoai, A. D. Van, and Q. N. Minh, “An integrating computing framework based on edge-fog-cloud for internet of healthcare things applications,” *Internet of Things (Netherlands)*, vol. 23, p. 100907, Oct. 2023, doi: 10.1016/j.iot.2023.100907.

[18] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, “Cybersecurity and healthcare: How safe are we?,” *BMJ*, vol. 358, p. j3179, Jul. 2017, doi: 10.1136/bmj.j3179.

[19] M. Kiruthika and T. Poongodi, “Investigation of Security Attacks in IoMT Devices and Federated Learning as a Mitigation Strategy,” *Procedia Computer Science*, vol. 258, pp. 3426–3435, 2025, doi: 10.1016/j.procs.2025.04.599.

[20] R. A. Jegatheswaran, I. J. Sakira, and N. A. A. Rahman, “A Review on IoMT device Vulnerabilities and Countermeasures,” *Journal of Physics: Conference Series*, vol. 1712, no. 1, pp. 1–12, Dec. 2020, doi: 10.1088/1742-6596/1712/1/012020.

[21] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, “Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security,” *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718, Jun. 2021, doi: 10.1109/JIOT.2020.3045653.

[22] A. Prasanth, L. D, R. K. Dhanaraj, S. P. C, and B. Balusamy, “Cognitive Computing for Internet of Medical Things,” in *Boca Raton: Chapman and Hall/CRC*, 2022, doi: 10.1201/9781003256243.

[23] N. H. Imam, “Adversarial Examples on XAI-Enabled DT for Smart Healthcare Systems,” *Sensors*, vol. 24, no. 21, pp. 1–23, Oct. 2024, doi: 10.3390/s24216891.

[24] X. Ma *et al.*, “Understanding adversarial attacks on deep learning based medical image analysis systems,” *Pattern Recognition*, vol. 110, pp. 1–11, Feb. 2021, doi: 10.1016/j.patcog.2020.107332.

[25] A. Selvakkumar, S. Pal, and Z. Jadidi, “Addressing Adversarial Machine Learning Attacks in Smart Healthcare Perspectives,” in *Lecture Notes in Electrical Engineering*, vol. 886, pp. 269–282, 2022, doi: 10.1007/978-3-030-98886-9_21.

[26] A. Alexei, N. Platon, I. Bolun, and A. Alexei, “Smart and Digital Healthcare. Advanced Technologies and Security Issues,” in *Proceedings of the Central and Eastern European eDem and eGov Days 2024*, New York, NY, USA: ACM: ACM, Sep. 2024, pp. 288–294, doi: 10.1145/3670243.3673857.

[27] S. F. Abed, S. Allain-Ioos, and N. Shindo, “Examining the threat of cyber-attacks on health care during the COVID-19 pandemic,” Iris WHO 2024, [Online]. Available: https://iris.who.int/bitstream/handle/10665/375831/WER9904-25-37.pdf. (Accessed: Sep. 11, 2024).

[28] Healthcare Information and Management Systems Society, “2023 HIMSS Healthcare Cybersecurity Survey,” HIMSS, 2024, [Online]. Available: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey. (Accessed: Sep. 01, 2024).

[29] Ponemon Institute, “Cyber insecurity in healthcare,” Proofpoint, 2024, [Online]. Available: https://www.proofpoint.com/us/cyber-insecurity-in-healthcare. (Accessed: Sep. 07, 2024).

[30] Verizon, “2024 Data Breach Investigations Report,” Verizon, 2024, [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2024/industries-intro/healthcare-data-breaches/. (Accessed: Oct. 07, 2024).

BIOGRAPHIES OF AUTHORS

Arina Alexei is an Associate Professor at the Department of Software Engineering and Automatics, Technical University of Moldova, since 2006. She obtained her Ph.D. degree in the field of Cybersecurity from the same university. Currently, she is a lecturer and researcher at the Faculty of Computers, Informatics and Microelectronics, Technical University of Moldova. Her main research interests include cybersecurity in various environments, particularly in educational systems, healthcare infrastructures, and small and medium-sized enterprises (SMEs). She can be contacted at email: arina.alexei@tse.utm.md.

Ion Bolun received his Ph.D. degree in Computer Science and his Doctor Habilitate degree in Information Technologies. He is a Full Professor and Doctor Habilitate at the Department of Software Engineering and Automation, Technical University of Moldova. His main fields of expertise include information systems, cybersecurity, and digital infrastructure resilience. Throughout his academic career, he has coordinated multiple national and institutional research projects and published extensively in peer-reviewed journals and international conferences. He can be contacted at email: ion.bolun@isa.utm.md.

Anatolie Alexei is a Ph.D. candidate in the specialty "Information Security Systems" and currently serves as a researcher and university lecturer at the Department of Telecommunications and Electronic Systems, Technical University of Moldova. His main areas of interest include cybersecurity, information system protection, and secure digital infrastructures. He is actively involved in scientific research focused on emerging threats, applied cryptography, and cybersecurity solutions for critical sectors, including healthcare and telecommunications. In the current paper, he contributed to the investigation, validation, data analysis, and manuscript preparation. He can be contacted at email: anatolie.alexei@adm.utm.md.