# PATIENT SAFETY IN THE DIGITAL REALITY: CHALLENGES AND PROSPECTS

# SIGURANȚA PACIENTULUI ÎN CONDIȚIILE REALITĂȚII DIGITALE

**Constantin PISARENCO**
ORCID ID: 0000-0001-5548-4653
Email:constantin.pisarenco@gmail.com
Free International University of Moldova

**CZU: 342.738:616-052:004** **DOI:** https://doi.org/10.59295/ssdoed2025.36

***Rezumat:*** *Actualitatea cercetării constă în faptul că digitalizarea rapidă a sănătății aduce noi provocări în ceea ce privește protecția pacienților, în special în domeniul securității cibernetice și al confidențialității datelor.*

*Scopul studiului este de a identifica principalele provocări asociate cu siguranța pacienților în contextul medicinei digitale și de a formula propuneri pentru îmbunătățirea siguranței și eficienței utilizării tehnologiilor digitale în sănătate.*

*Material și metode. Cercetarea a utilizat metode de analiză a aspectelor juridice și tehnice legate de aplicarea tehnologiilor digitale în sănătate, cu accent pe evaluarea riscurilor și identificarea soluțiilor de minimizare a acestora.*

*Rezultate. Digitalizarea a îmbunătățit calitatea asistenței medicale, dar a evidențiat riscuri, precum atacurile cibernetice și scurgerile de date.*

*Concluzii. Protecția pacienților necesită o abordare integrată, inclusiv îmbunătățirea reglementărilor legale și formarea personalului, toate acestea fiind esențiale pentru succesul pe termen lung.*

***Cuvinte-cheie:*** *siguranța pacienților, medicina digitală, riscuri.*

***Abstract:*** *The relevance of the research lies in the fact that the rapid digitalization of healthcare brings new challenges in terms of patient protection, especially in the field of cybersecurity and data privacy.*

*The aim of the study is to identify the main challenges associated with patient safety in the context of digital medicine and to formulate proposals for improving the safety and efficiency of the use of digital technologies in healthcare.*

*Material and methods. The research used methods of analyzing legal and technical aspects related to the application of digital technologies in healthcare, with a focus on assessing risks and identifying solutions to minimize them.*

*Results. Digitalization has improved the quality of healthcare, but has highlighted risks, such as cyberattacks and data leaks.*

*Conclusions. Patient protection requires an integrated approach, including improving legal regulations and staff training, all of which are essential for long-term success.*

***Keywords**: patient safety, digital medicine, risks.*

## Introduction

The digitalization of healthcare represents one of the most significant transformations in modern medicine, encompassing a wide range of technologies, including electronic medical records, telemedicine, artificial intelligence, wearable devices, and more. These innovations contribute to increasing the efficiency of medical care, improving the interaction between patients and doctors, and enabling more accurate diagnostics and personalized treatment. However, alongside these advantages, a whole set of new challenges emerges, particularly concerning patient safety, which extends beyond the traditional medical context to include aspects such as data protection, cybersecurity, and the ethical use of technologies.

In this regard, it is of particular importance to study the existing risks and potential threats, assess their impact on the quality of medical care, and develop recommendations that can help minimize these risks and enhance patient safety in the rapidly evolving digital reality [11, 12, 13].

The aim of this study is to identify and systematize the main challenges related to patient safety in the context of digital medicine, as well as to develop proposals for improving the safety and efficiency of digital technology usage in healthcare.

## Materials and Methods

The search for scientific articles and publications was conducted using the PubMed, Google Scholar, and Scopus databases, as well as open internet sources. Methods of analyzing legal and technical aspects of digital technologies in healthcare were applied, with a focus on risk assessment and strategies for their mitigation. An analysis was conducted on international and national regulations governing the use of digital technologies and their impact on patient safety.

**Results and Discussion**

The digital reality, representing the complete digitalization of medicine, encompasses all aspects of medical care—from diagnosis and treatment to patient data management and interaction. In these conditions, ensuring patient safety becomes a central task, requiring new approaches and solutions capable of addressing the challenges and threats associated with the digitalization of healthcare.

With the implementation of digital technologies in healthcare, issues of cybersecurity and data protection have gained paramount importance. Patient medical data contains a vast amount of confidential information, including diagnoses, medical history, test results, prescribed medications, and other sensitive data. Leaks of such information can have serious consequences for both the patient and the medical institution, including loss of patient trust, legal sanctions, and reputational risks.

Digital technologies, such as electronic medical records (EMR), telemedicine, and AI-based decision support systems, enhance diagnosis, expedite treatment processes, and improve the quality of medical services. However, integrating these technologies into existing medical processes poses a complex challenge. Moreover, the implementation of digital technologies requires significant investment in training medical personnel.

Despite the numerous advantages, such as increased accessibility and efficiency of medical care, the digitalization of medicine is associated with technical, legal, ethical and clinical risks that can significantly impact the quality and safety of medical services.

Technical risks in the use of digital technologies in medicine are related to the application of equipment, software, and telecommunications technologies that facilitate interaction between doctors, patients, and medical systems. One of the primary technical risks is the instability of internet connections, which can lead to data distortion, delays in information transmission, or complete loss of connectivity. For instance, in rural and remote areas, where access to high-speed internet is limited, telemedicine and other digital medical services may be unreliable, reducing their effectiveness and safety.

There are also risks associated with the use of malfunctioning or outdated equipment. Medical devices and software used to monitor patient conditions must be accurately calibrated and meet established standards. Otherwise, diagnostic errors may occur, potentially leading to incorrect treatment.

Data security risks also play a crucial role among technical risks. In the context of digital interactions between patients and medical institu-

tions, there is a need to protect personal data from unauthorized access and cyberattacks. Data security breaches can lead to the leakage of confidential information, which in turn may result in legal consequences and loss of patient trust in digital medical services.

Legal risks in the use of digital technologies in medicine are associated with the need to comply with legislation regulating the provision of medical services using digital means. One of the key legal risks is the blurring of responsibility boundaries between healthcare professionals and platforms using digital technologies. Another important aspect of legal risks concerns compliance with licensing and certification requirements for medical professionals using digital technologies.

Ethical risks include concerns about ensuring equal access to medical services. In the context of digital inequality, where not all patients have equal access to technology, there is a risk of unequal access to medical care. Additionally, remote interactions might lead to violations of traditional medical ethics, such as ensuring full informed consent from the patient [6].

Clinical risks are among the most significant when using digital technologies in medicine, as they directly relate to the safety and quality of medical care. One of the primary clinical risks is the possibility of incorrect diagnosis due to the limitations of remote interactions and the use of automated systems. When using digital technologies, a physician may rely on information provided by the patient or data obtained from medical devices and software, which can lead to inaccurate conclusions.

To mitigate the risks associated with the use of digital technologies in medicine, it is necessary to implement comprehensive measures aimed at improving the quality and safety of the services provided. From a technical standpoint, this may include improving communication infrastructure, using modern and certified medical devices and software, and implementing strict data security protocols.

To reduce clinical risks, it is essential to develop protocols aimed at enhancing the accuracy of diagnosis and treatment in digital medicine. This could involve using high-quality images and videos, training healthcare professionals in the specifics of working with digital technologies, and integrating digital solutions with traditional medical methods for a comprehensive approach to patient care.

From a legal perspective, it is necessary to develop and implement unified standards and protocols that regulate the responsibilities of healthcare professionals and platforms using digital technologies. It is also crucial to ensure uniform licensing and certification requirements

for healthcare professionals, which would eliminate legal uncertainty and improve access to medical services.

The European Union (EU) is a leader in developing regulations aimed at protecting personal data, including medical information. The General Data Protection Regulation (GDPR), which came into effect in 2018, is one of the most comprehensive data protection systems in the world. GDPR imposes strict requirements on the collection, processing, and storage of data and grants EU citizens extensive rights to access and control their information.

GDPR requires medical institutions not only to adhere to core data protection principles, such as data minimization and ensuring data security, but also to notify regulatory authorities and affected individuals of any data breaches within 72 hours. This requirement facilitates a more rapid response to incidents and increases the accountability of medical institutions for the security of patient data [5].

Additionally, the EU is actively working on creating a unified digital market, which includes initiatives to enhance cybersecurity in healthcare. In 2020, the European Commission adopted the Cybersecurity Strategy for the Digital Decade, which aims to strengthen the protection of critical infrastructure, including healthcare systems, and improve the cybersecurity resilience of medical institutions [4].

After leaving the European Union, the United Kingdom retained the main provisions of the GDPR in its national legislation by adopting the Data Protection Act 2018. However, unlike the EU, the UK has adopted a more flexible approach to regulating AI (Artificial Intelligence—Authors' note) and other digital technologies, allowing for faster innovation in healthcare [10].

The United States has one of the most developed legal frameworks for protecting medical data. The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, is the primary legislation governing the protection of medical information in the U.S. HIPAA imposes strict requirements for the confidentiality and security of patient data, including mandatory data encryption, restricted access to information, and mandatory breach notifications [7].

In addition to HIPAA, the 21st Century Cures Act, passed in 2020, includes provisions aimed at ensuring the interoperability of digital medical systems and the accessibility of patient data [1]. And in 2019, the FDA released the "Guidance on Clinical Decision Support Software", which includes recommendations on the use of AI for clinical decision support. These recommendations are aimed at ensuring the safety and effectiveness of AI systems, as well as minimizing the risks associated with their use [14].

To ensure patient safety in the digital era, it is essential to develop and implement unified international security standards for the use of digital technologies in medicine. These standards should cover all aspects of handling patient data, including its collection, processing, storage, and transmission. A crucial step in this direction is the harmonization of national legislation with international norms, such as ISO/IEC 27001:2013, which establishes general requirements for information security management [8].

Moreover, standards for the use of AI in healthcare need to be developed. These standards should address both technological aspects (e.g., accuracy and reliability requirements of algorithms) and ethical aspects (e.g., transparency and explainability of AI-driven decisions). The International Organization for Standardization (ISO) has already begun working on such standards, which is a significant step toward the global adoption of safe AI technologies in medicine [9].

Training medical personnel is a key element in ensuring patient safety in the digital age. Healthcare professionals must not only be proficient in using new technologies but also understand their limitations and the potential risks associated with their use. This necessitates the development of training programs that encompass not only technical aspects but also issues of ethics, privacy, and cybersecurity.

International organizations, such as the World Health Organization and the European Commission, play an important role in this process by developing guidelines for training healthcare personnel in digital skills [2, 15].

Additionally, universities and educational institutions must adapt their curricula to the new realities of digital medicine. This includes integrating courses on cybersecurity, AI, and data management into the training programs for future doctors and healthcare workers.

The creation of monitoring and analysis systems for cyber threats is critically important for ensuring patient safety. These systems should not only be able to detect and prevent cyberattacks but also respond to them quickly to minimize damage. This requires the use of advanced technologies such as machine learning and big data analytics to predict potential threats and develop measures to neutralize them.

Another important aspect is the development of incident response scenarios. Medical institutions must have clear action plans in case of cyberattacks, including procedures for data recovery, patient notifications, and interactions with regulatory authorities. National governments and international organizations can play a significant role in developing such plans and adapting them to specific conditions [3].

Regular audits and testing of security systems are also an integral part of a patient safety strategy. They allow for the identification of vulnerabilities and timely measures to address them, significantly reducing the risks of cyberattacks and data breaches.

## Conclusion

The digital transformation of healthcare presents remarkable opportunities for enhancing medical care quality, yet it introduces significant challenges that threaten patient safety. This analysis identified the key risks associated with digital technologies in medicine, spanning technical, legal, ethical, and clinical dimensions. Ensuring patient safety in the digital era demands a comprehensive approach to mitigating these risks. Technical vulnerabilities, such as cyberattacks and system incompatibilities, necessitate robust data protection measures and the regular testing of technologies. Legal risks, particularly those related to liability and data protection compliance, require the development of clear regulations and protocols. Ethical concerns, including inequities in technology access and the use of patient data, call for transparency and adherence to informed consent principles. Clinical risks, stemming from potential diagnostic or treatment errors, emphasize the need for reliable protocols and thorough training for healthcare professionals in digital systems. By addressing these multifaceted challenges, the healthcare sector can fully leverage the benefits of digital medicine while safeguarding patient safety at every stage of care.

**References:**

1. 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2020). Available at: https://www.govinfo.gov/content/pkg/PLAW-114publ255/pdf/PLAW-114publ255.pdf [Accessed 18.08.2024].
2. European Commission. (n.d.). Digital Skills and Jobs. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-skills-and-jobs [Accessed 18.08.2024].
3. European Union Agency for Cybersecurity (ENISA). (2020). Cybersecurity in the Healthcare Sector. Available at: https://www.enisa.europa.eu/publications/cybersecurity-in-healthcare [Accessed 18.08.2024].
4. European Union Agency for Cybersecurity (ENISA). (2020). Consolidated Annual Activity Report 2020. Available at: https://www.enisa.europa.eu/publications/corporate-documents/enisa-consolidated-annual-activity-report-2020 [Accessed 18.08.2024].

5. European Union. (2016). General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/ [Accessed 18.08.2024].
6. GREENHALGH, T., WHERTON, J., SHAW, S., & MORRISON, C. (2020). Video consultations for COVID-19: A rapid assessment in primary care. BMJ, 368, m998. Available at: https://www.bmj.com/content/368/bmj.m998 [Accessed 18.08.2024].
7. Health Insurance Portability and Accountability Act (HIPAA). (1996). Available at: https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996/ [Accessed 18.08.2024].
8. ISO/IEC. (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. Available at: https://www.iso.org/isoiec-27001-information-security.html [Accessed 18.08.2024].
9. ISO/IEC JTC 1/SC 42. (n.d.). Artificial Intelligence. International Organization for Standardization. Available at: https://www.iso.org/committee/6794475.html [Accessed 18.08.2024].
10. National Cyber Security Centre. (2021). Cyber Essentials Scheme: Requirements for IT infrastructure. UK. Available at: https://www.ncsc.gov.uk/cyberessentials/overview [Accessed 18.08.2024].
11. PRICE, W. N., & COHEN, I. G. (2019). Privacy in the age of medical big data. Nature Medicine, 25(1), 37-43. Available at: https://www.nature.com/articles/s41591-018-0272-7 [Accessed 18.08.2024].
12. RAJKOMAR, A., DEAN, J., & KOHANE, I. (2019). Machine learning in medicine. New England Journal of Medicine, 380(14), 1347-1358. Available at: https://www.nejm.org/doi/full/10.1056/NEJMra1814259 [Accessed 18.08.2024].
13. TOPOL, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine, 25(1), 44-56. Available at: https://www.nature.com/articles/s41591-018-0300-7 [Accessed 18.08.2024].
14. U.S. Food and Drug Administration. (2019). Guidance on Clinical Decision Support Software. Available at: https://www.fda.gov/media/109618/download [Accessed 18.08.2024].
15. WHO. (2019). Guideline Recommendations on Digital Interventions for Health System Strengthening. Geneva: WHO. Available at: https://www.ncbi.nlm.nih.gov/books/NBK541902/ [Accessed 18.08.2024].