C.Z.U.: 614.2:34:004.9
DOI: https://doi.org/10.52692/1857-0011.2024.3-80.12

THE THREE PILLARS OF LEGAL PROTECTION FOR DOCTORS IN THE ERA OF DIGITAL MEDICINE: PROTOCOLS, DOCUMENTATION, CONSENT

[1]**Constantin PISARENCO,** Dr. of Laws, Associate Professor,
[2]**Serghei PISARENCO,** Dr. hab. in medical sciences, Associate Professor

[1]Free International University of Moldova, Chisinau, Republic of Moldova
[2]Institute of Phthisiopneumology "Chiril Draganiuc", Chisinau, Republic of Moldova

e-mail: *constantin.pisarenco@gmail.com*

Summary.

This article explores the primary legal aspects of physician protection in the context of digital medicine. It examines three key elements of legal defense for doctors — clinical protocols, medical documentation, and informed consent. Legal risks associated with the use of electronic systems are discussed, along with recommendations to minimize liability. The author also addresses issues of data privacy and the use of telemedicine technologies, emphasizing the need for legal regulation and security standards in the digital environment.

Keywords: digital medicine, legal protection for doctors, clinical protocols, medical documentation, informed consent, telemedicine, data privacy.

Rezumat. Cele trei elemente esențiale de protecție juridică a medicului în epoca medicinei digitale: protocoale, documentație, consimțământ.

Articolul examinează principalele aspecte juridice ale protecției medicilor în contextul medicinei digitale. Sunt analizate trei elemente cheie de protecție juridică — protocoalele clinice, documentația medicală și consimțământul informat voluntar. Sunt prezentate riscurile juridice asociate utilizării sistemelor electronice și sunt propuse recomandări pentru minimizarea litigiilor juridice. Autorul subliniază, de asemenea, problemele legate de confidențialitatea datelor și aplicarea tehnologiilor de telemedicină, subliniind importanța reglementărilor și standardelor de securitate în mediul digital.

Cuvinte cheie: medicină digitală, protecție juridică a medicului, protocoale clinice, documentație medicală, consimțământ informat, telemedicină, confidențialitatea datelor.

Резюме. **Три кита юридической защиты врача в эпоху цифровой медицины: протоколы, документация, согласие.**

В статье исследуются основные правовые аспекты защиты врача в условиях цифровой медицины. Рассматриваются три ключевых элемента юридической защиты врача — клинические протоколы, медицинская документация и добровольное информированное согласие. Анализируются правовые риски, связанные с использованием электронных систем, и предлагаются рекомендации для минимизации юридических претензий. Особое внимание уделено вопросам конфиденциальности данных и применения телемедицинских технологий, подчеркивая важность правового регулирования и стандартов безопасности в цифровой среде.

Ключевые слова: цифровая медицина, юридическая защита врача, клинические протоколы, медицинская документация, информированное согласие, телемедицина, конфиденциальность данных.

Introduction.

Modern medicine is being actively transformed by digital technology, driven by advances in information technology, increased patient data, and accelerated exchange of medical information. This contributes to improved diagnosis and treatment, but also creates many legal challenges for physicians and medical organizations. In the context of digital medicine, the issues of physician legal defense become particularly relevant, as the risk of errors, data breaches, and legal disputes increases with the transition to electronic medical record systems and work protocols. Each of these risks requires detailed analysis and consideration in the work of medical personnel, as errors in the maintenance of electronic records or violation of regulations can lead to significant legal consequences for doctors and medical institutions.

The rapid development of telemedicine technologies, as part of digital transformation, makes it possible to provide medical care remotely, which is especially important when traditional methods of interaction with patients are limited (e.g., during pandemics or for patients in remote regions). However, the legal regulation of telemedicine is still in its infancy, which causes certain difficulties for physicians providing care at a distance. Such aspects as consent to remote treatment, digital storage of patient data and liability for remote treatment require revision and adaptation of existing legal norms to the realities of the digital age.

Physician compliance with clinical protocol standards is also important, as they are gradually being integrated into digital systems and made available for use through electronic databases and mobile applications. This change reduces decision-making time and increases the likelihood of providing quality care. However, in the absence of clear regulation, the use of digital protocols may expose the physician to legal risks, especially if the use of such protocols varies from traditional practice. Therefore, there is a need for unified standards and recommendations for physicians in the context of digital medicine, as well as additional legal measures aimed at protecting the rights and obligations of medical professionals.

The purpose of this study is to analyze three key aspects of physician legal protection in digital medicine: adherence to clinical protocols, medical record keeping, and obtaining patient informed consent.

Material and methods.

The study is based on the analysis of legal, clinical and ethical aspects of the use of digital technologies in medicine. The main sources of data were international legal acts, clinical protocols and academic publications. The methodology includes comparative analysis of regulatory frameworks, practices of digital systems and current recommendations for their use in different countries.

Results and discussion.

National clinical protocols as a basis for legal protection of the physician

Clinical protocols are standardized algorithms for diagnosis and treatment based on the principles of evidence-based medicine. They contribute to the unification of approaches to medical care, minimizing risks for the patient and providing legal protection for the doctor. Protocols are developed on the basis of current scientific data, recommendations of international organizations and the results of clinical trials.

From a legal standpoint, adherence to clinical protocols provides the physician with clear guidelines and reduces the likelihood of errors. In the case of litigation, documented adherence to protocols confirms compliance with standards of care. In addition, protocols help regulatory agencies to assess the quality of medical services, reducing the subjective responsibility of the doctor and focusing on objective standards.

Electronic databases make clinical protocols available to clinicians in real time, simplifying clinical decision-making. The integration of digital protocols with data processing systems allows for the automation of many processes, which increases their efficiency. However, this comes with new challenges, such as the need to update data, protection of confidential information and technical failures.

The transition to digital formats requires additional legal regulation to prevent errors related to outdated data or misapplication of protocols. Healthcare providers should consider cybersecurity requirements to minimize the risks of data breaches and legal claims.

The introduction of telemedicine technologies has changed the approach to the application of clinical protocols. In remote treatment settings, protocols must adapt to the peculiarities of remote diagnosis, where there is no physical contact with the patient. This creates additional legal and ethical risks, including issues of data protection and evidencebased telemedicine consultations.

The privacy of data transmitted through digital channels is a key aspect. The use of platforms that comply with international security standards (e.g., HIPAA or GDPR) helps minimize the risks of information leaks and legal consequences.

The format of telemedicine consultations differs from traditional face-to-face interaction, which requires the development of special legal norms regulating this process. One of the main problems is the choice of clinical protocols for remote diagnostics, where the physician's capabilities are limited by technical means of communication. Protocols used in telemedicine are not yet sufficiently unified, which creates uncertainty and legal risks for doctors.

Telemedicine raises issues of legal liability, especially in cases where remote consultation results in inaccurate diagnosis or inadequate treatment. Limitations of technical means, such as poor communication quality or limited access to the patient's medical data, may increase the risk of errors. These features should be taken into account in the development of legal norms to ensure the protection of the physician from unjustified claims, as well as the patient's right to quality care.

With the advancement of artificial intelligence technology in medicine, doctors have the opportunity to use algorithms and machine learning to diagnose and optimize treatment. AI is capable of analyzing huge amounts of medical data, offering solutions based on the analysis of various factors. However, in terms of legal protection of the physician, the use of AI is associated with a number of legal risks and unresolved issues.

One key issue is the allocation of liability for errors associated with AI recommendations. For example, if a physician makes a decision based on an algorithm's recommendations, legal liability for potential consequences can be a matter of debate. Many AI algorithms remain black boxes, which makes them difficult to interpret and causes difficulties in determining the source of error.

Careful quality control of AI algorithms is required to minimize legal risks. Unlike traditional clinical protocols, AI algorithms can be subject to biases of the data on which they were trained. This can lead to inappropriate recommendations if the algorithms have not been customized for a specific patient population. Certification and standardization of AI algorithms are becoming essential for their safe use in medical practice.

AI requires processing large amounts of data, including sensitive patient information. Violations of data protection standards can lead to legal consequences such as fines and loss of patient trust. Compliance with regulations such as GDPR and HIPAA plays a key role in ensuring the legality of AI in healthcare.

Medical records as a legal instrument

Medical records play a central role in a physician's legal defense, recording all aspects of patient interaction, from complaints and symptoms to treatment and prescriptions. Strict adherence to record-keeping standards is not only an essential element in ensuring proper patient care, but also an effective means of protecting the physician from legal claims. Legislation in most countries contains clear requirements for the maintenance, storage and access to medical data, compliance with which helps to prevent legal disputes.

Prior to the digital age, record keeping was predominantly paper-based, limiting rapid access to data and increasing the likelihood of errors or loss of records. The move to electronic medical records (EMRs) has standardized the recordkeeping process and improved control over the completeness and accuracy of records.

Electronic systems allow for the creation of time-stamped records with a history of changes, which greatly increases a physician's legal protection. For example, in the event of a dispute, it can be proven that the record was made in a timely manner and according to established standards. In addition, EMRs facilitate integration with reminder systems and provide physicians with structured data that minimizes the likelihood of missing important information.

Despite the obvious benefits, the digitalization of medical records comes with a number of risks, including threats of cyberattacks and unauthorized access to patient data. This makes data protection a critical concern for healthcare providers. In countries with strict privacy standards, such as GDPR in the EU and HIPAA in the U.S., security breaches can result in significant fines and damage to the reputation of a healthcare organization.

With the development of telemedicine and artificial intelligence (AI) technologies, there is a need to adapt medical record keeping standards to the new format. Proper documentation of remote consultations, including patient consent and description of procedures performed, is becoming a key aspect of legal protection. Digital technologies make it possible to record remote interactions using video recordings and time stamps, which makes it easier to prove compliance with standards.

AI opens up new opportunities for automating medical record keeping. Modern algorithms can process data from medical devices, analyze patient history, and even suggest optimal treatment options to doctors. This reduces the burden on physicians and increases the accuracy of records.

The use of AI in documentation requires adherence to strict privacy and data protection standards, as algorithms need large amounts of personal information. Failure to comply with standards such as HIPAA or GDPR can have significant legal consequences. In addition, there is the question of legal liability for mistakes made when using AI, especially if the algorithm operates as a black box and its recommendations are difficult to explain.

Voluntary informed consent of the patient as a protection of the doctor's interests

Voluntary informed consent of the patient is a key element of medical practice that protects the rights of the patient and the interests of the physician. This process involves the patient voluntarily agreeing to medical procedures, recognizing the possible risks, available alternatives and likely outcomes. Legally informed consent ensures that the physician respects the patient's autonomy by providing the patient with complete and accurate information about the planned intervention.

From a legal point of view, informed consent protects the physician from being accused of violating the patient's rights. This is particularly important in cases where the medical intervention involves a high risk or uncertain outcome. The absence of such consent leaves the physician vulnerable to claims by the patient or the patient's representatives. Thus, the process of informing and obtaining consent becomes a central aspect of a physician's legal defense.

In traditional medical practice, the process of obtaining informed consent consisted of signing a paper form where the patient confirmed his or her consent to the procedure. Often these forms contained standardized language and were not tailored to specific procedures, creating a risk of legal challenge. If the patient claimed that the information received was insufficient, this could lead to litigation.

In addition, paper forms created difficulties in storing and accessing documents. If they were lost, the doctor would lose evidence that the patient had been properly informed. This emphasized the need for more reliable and modern methods of documentation.

With the development of digital technology, the consent process has become more efficient. Electronic systems can capture patient consent digitally, including time stamps and proof of familiarization. This reduces the likelihood of data loss and provides easy access to data when needed. Current methods include the use of video and interactive systems that make the process more informative and transparent.

Digital methods also contribute to the physician's defense by capturing every step of the consent process. For example, the use of video recordings or interactive interfaces makes it possible to prove that the patient was informed in detail about the risks and gave consent knowingly. However, digitalization also brings new challenges related to the protection of patient data and compliance with legal requirements such as GDPR and HIPAA.

With the development of telemedicine and artificial intelligence (AI) technologies, the consent process has taken on new dimensions. Remote consultations require that the patient's consent to the use of digital technologies and remote therapies be recorded. It is important that the patient is aware of the limitations and risks of telemedicine, including data protection and possible limitations on diagnostic capabilities.

Clinicians need to pay special attention to patient information in remote consultation settings. Since there is no face-to-face interaction, more effort is required to ensure that the patient understands all aspects of treatment. This reduces the likelihood of legal disputes and strengthens the patient's trust in the physician.

The use of AI technologies in medicine has made the informed consent process more complex, as patients need to understand not only the medical aspects of treatment, but also the specifics of AI applications. Modern AI systems are used for diagnosis, prognosis and clinical decision-making, which requires physicians to explain to patients the role of AI and the associated risks and limitations. Patient education about the transparency and safety of AI use is becoming an important element.

Conclusion.

In the era of digitalization of medicine, the legal protection of the physician takes on new forms related to the use of clinical protocols, medical record keeping and the informed consent process. These three aspects - protocols, documentation and consent – ensure the legal stability of the physician and minimize legal risks. The transition to electronic systems, telemedicine and AI offer new opportunities to improve the efficiency of medical care, but require legal revisions and increased regulation.

Future legal measures should be tailored to the specifics of digital tools, ensuring robust protection for physicians and patients. This includes standardizing protocols, ensuring data security and introducing clear norms for the use of AI in medicine. Only a comprehensive approach to regulation will enable successful adaptation to the challenges of the digital age.

In the era of digitalization of medicine, physicians should use up-to-date electronic clinical protocols to minimize errors and strengthen legal protections. Certified AI systems should be utilized, capturing patient consent and clarifying the role of AI in treatment. Time-stamped electronic systems can monitor adherence to standards and provide evidence in case of disputes. It is also important to educate patients in detail about the risks and limitations of digital technologies and record the process of clarification to mitigate legal risks.

Bibliography.

1. Abujaber A.A., Nashwan A.J. *Ethical Framework for Artificial Intelligence in Healthcare Research: A Path to Integrity*. World J. Methodol., 2024; 14(3):94071. doi:10.5662/wjm.v14.i3.94071.
2. Amann J., et al. *Explainability for Artificial Intelligence in Healthcare: A Multidisciplinary Perspective*. BMC Med. Inform. Decis. Mak., 2020; 20(1):310. doi:10.1186/s12911-020-01332-6.
3. *Applications and Challenges of Telemedicine: Privacy-Preservation as a Case Study*. Arch. Iran. Med., 2023; 26(11):654-661. doi:10.34172/aim.2023.96.
4. Beauchamp T.L., Childress J.F. *Principles of Biomedical Ethics*. Oxford Univ. Press, 2019. www.oxfordbiomedicalethics.com.
5. Berg J.W., et al. *Informed Consent: Legal Theory and Clinical Practice*. Oxford Univ. Press, 2019. www.oxfordinformedconsent.com.

6. Coventry L., Branley D. *Cybersecurity in Healthcare: A Narrative Review of Trends, Threats, and Ways Forward*. Maturitas, 2018; 113:48-52. doi:10.1016/j.maturitas.2018.04.008.
7. Garcia E., et al. *Telemedicine Law and International Clinical Protocols: Challenges and Prospects*. Int. J. Health Law Policy, 2021; 22(4):112-130. www.healthlawpolicyjournal.com/protocols.
8. *e-Consent: A Complete Guide*. Conduct Science, www.conductscience.com/digital-health/e-consent/.
9. *Electronic Health Records Explained*. ISO, www.iso.org/healthcare/electronic-health-records.
10. European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*. Off. J. Eur. Union, 2016; 59(119):1-88. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.
11. Kruse C.S., et al. *Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends*. Technol. Health Care, 2017; 25(1):1-10. doi:10.3233/THC-161263.
12. Langarizadeh M., Moghbeli F., Aliabadi A. *Application of Ethics for Providing Telemedicine Services and Information Technology*. Med. Arch., 2017; 71(5):351-355. doi:10.5455/medarh.2017.71.351-355.
13. Nofianto E. *The Legal Protection of Patients as Victims of Medical Malpractice by Physicians on Telemedicine Services*. Int. J. Law Stud., 2023; 1(3):57-71. doi:10.62951/ijls.v1i3.57.
14. Obermeyer Z., Emanuel E.J. *Predicting the Future: Big Data, Machine Learning, and Clinical Medicine*. N. Engl. J. Med., 2016; 375(13):1216-1219. doi:10.1056/NEJMp1606181.
15. Palaniappan K., Lin E.Y.T., Vogel S. *Global Regulatory Frameworks for the Use of Artificial Intelligence in the Healthcare Services Sector*. Healthcare (Basel), 2024; 12(5):562. doi:10.3390/healthcare12050562.
16. Panter M. *Potential Legal Implications of Telemedicine and Telehealth*. Am. Bar Assoc., www.americanbar.org/groups/law_practice/resources/law-technology-today/2021/implications-of-telemedicine-and-telehealth/.
17. Tikkinen-Piri C., Rohunen A., Markkula J. *EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies*. Comput. Law Secur. Rev., 2018; 34(1):134-153. doi:10.1016/j.clsr.2017.05.015.
18. United States, Department of Health and Human Services. *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Public Law 104-191, 1996. www.hhs.gov/hipaa/index.html.