ISSN 2524 – 0684 e-ISSN 2524 – 0692

UDC 340.13:614.2(574)
IRSTI 10.09.01
DOI: 10.53065/kaznmu.2025.73.2.006

Поступил в редакцию: 03.06.2025
Принято к публикации: 20.06.2025

MEDICAL CONFIDENTIALITY IN THE LEGAL SYSTEM OF KAZAKHSTAN: IS IT A REAL TOOL FOR PROTECTING PATIENTS' PRIVATE LIFE?

S.T. IKSATOVA, B.Sh. BEKBATYROV

Innovative University of Eurasia, Pavlodar, Kazakhstan

Abstract

Introduction. Medical confidentiality is one of the key elements in protecting patients' personal data and ensuring their right to privacy. In the context of healthcare digitalization and the expanding powers of government authorities in Kazakhstan, new challenges arise concerning the confidentiality of medical information.

Aim. This article aims to analyze the legal regulation of medical confidentiality in the Republic of Kazakhstan, identify existing legislative gaps and threats to medical data confidentiality, and develop proposals for improving law enforcement practices.

Materials and methods. The study employs methods of comparative legal analysis, systemic and normative approaches, allowing an assessment of the compliance of current regulations with international standards (GDPR, HIPAA). Additionally, content analysis of Kazakhstan's regulatory legal acts and judicial practice was conducted.

Results. It has been established that Kazakhstan's legislation formally ensures the protection of medical confidentiality; however, it contains several exceptions that allow government agencies to request personal medical data without patient consent. Significant issues include the vagueness of national security criteria, insufficient regulation of access to digital medical databases, and the lack of effective mechanisms for monitoring and notifying patients about the transfer of their data to third parties. Risks of data leaks have been identified due to the inadequate level of cybersecurity in medical information systems and the low awareness of patients about their rights.

Conclusion. To enhance the protection of medical confidentiality in Kazakhstan, reforms are needed in several areas: strengthening judicial oversight over requests for medical data disclosure, tightening criminal and administrative liability for unlawful dissemination, implementing transparency mechanisms and patient notifications, and improving cybersecurity standards. The development of educational programs for medical personnel and increasing patients' legal awareness are also crucial steps toward strengthening the institution of medical confidentiality and adapting it to the digital era.

Keywords: medical confidentiality, personal data, privacy, cybersecurity, right to private life, Kazakhstan, healthcare digitalization, medical information, legal regulation

Introduction. Physician-patient confidentiality has ancient historical roots, originating from the Hippocratic Oath, which emphasizes the physician's duty not to disclose information related to the patient's health status [1]. Over time, this obligation has received more systematic legal reinforcement, ranging from medieval medical statutes to modern constitutional norms and specialized healthcare laws [2-4].

ISSN 2524 – 0684 e-ISSN 2524 – 0692

In the Republic of Kazakhstan, the institution of physician-patient confidentiality is currently based on several key legal acts, one of the most fundamental being the Constitution of the Republic of Kazakhstan (1995, as amended) [5]. For example, Article 18 of the Constitution guarantees the inviolability of private life, personal and family secrets [5]. This provision, in turn, creates a fundamental legal basis for the subsequent detailed regulation of medical confidentiality [6]. Article 39 states that human rights and freedoms may be restricted exclusively by law and only to the extent necessary to protect the constitutional order, public order, human rights and freedoms, as well as public health and morality. Thus, state intervention in the field of personal medical information must be justified and legislatively regulated [7].

Another equally important legal act is the Code of the Republic of Kazakhstan "On people's health and the healthcare system" (2020) [6]. This is a fundamental act that systematizes the norms related to medical care, including compliance with and protection of medical confidentiality. Specifically, in chapters dedicated to patients' rights (e.g., Chapter 13), it is stated that medical workers are obliged to maintain the confidentiality of information about a patient's health condition and other data obtained during the provision of medical services (Articles 95–96). The Code also provides mechanisms for legal liability (civil, administrative, and criminal) in cases of breaches of medical confidentiality [8].

In addition to the above, the Law of the Republic of Kazakhstan "On Personal Data and Their Protection" dated May 21, 2013, No. 94-V, plays a significant role. It regulates the collection, storage, processing, dissemination, and protection of personal data, including particularly sensitive health data. For instance, Articles 7 and 8 of this law mandate obtaining the subject’s (patient’s) consent for the processing of their personal data, except in cases provided by law (e.g., upon request from law enforcement agencies or for the protection of the life and health of other individuals). Article 10 establishes general principles of security and confidentiality in handling personal data, which directly relates to compliance with medical confidentiality [9].

It is also important to note the Criminal Code of the Republic of Kazakhstan (CC RK), which contains provisions on criminal liability for the unlawful disclosure of information constituting medical secrecy, as well as for unauthorized collection and dissemination of personal data (Article 147 CC RK – violation of privacy, Article 192 CC RK – disclosure of private life information, etc.). These provisions regulate the responsibility of medical personnel and other individuals who have access to confidential information that may be unlawfully used for personal gain or other purposes [10].

Beyond the aforementioned legal sources, aspects of medical confidentiality are regulated by a number of subordinate acts, such as orders of the Ministry of Healthcare regarding the rules for maintaining medical records, as well as provisions on the procedure for exchanging information between medical organizations and state authorities [11]. Additional nuances may be reflected in laws affecting related areas, such as legislation on state statistics, social protection, and insurance [12].

However, despite the formal recognition of the special status of medical confidentiality [13], legal practice in Kazakhstan demonstrates a number of situations where medical secrecy can be disclosed without the patient's consent. For example, at the request of competent authorities (courts, prosecutors, investigative bodies) based on the Criminal Procedure Code of the Republic of Kazakhstan (CPC RK) [10], as well as in the interests of public safety and public health, including anti-epidemic measures [8].

When considering social security issues (such as pension and benefit assignments), authorized bodies may request information about a person's health status. Additionally, the operation of electronic platforms (EGov, digital medical record storage systems) may lead to

ISSN 2524 – 0684 e-ISSN 2524 – 0692

an expansion of the range of individuals and organizations with access to certain patient data [14-16].

In the scientific literature on medical law and bioethics, it is emphasized that an excessive number of exceptions allowing authorized structures to access confidential information creates a risk of "dilution" of the institution of medical secrecy [17]. Researchers note that patients are often unaware of how many different bodies and institutions have the authority to access their personal medical data and lack mechanisms for real control over the use of this information [18].

Thus, this article will analyze the legislative foundations of medical secrecy, focusing on the practical aspects of disclosing confidential information in the context of national security and criminal prosecution, as well as the risks associated with the digital transformation of healthcare in Kazakhstan. The aim of this review is to assess whether the existing regulatory system aligns with the principle of protecting the patient's right to privacy or, on the contrary, whether this right may, in some cases, lose its force under the pressure of state interests and bureaucratic procedures.

Materials and Methods. This study employs comprehensive legal analysis methods that enable a thorough assessment of the compliance of existing regulations with international standards (GDPR, HIPAA) and the identification of potential gaps in legal regulation.

Comparative Legal Analysis

This method was used to compare the norms of Kazakhstan’s national legislation with international standards in the field of personal data and medical information protection. Particular attention was paid to the European Union’s General Data Protection Regulation (GDPR) and the U.S. Health Insurance Portability and Accountability Act (HIPAA), including their key provisions on data protection, processing principles, data subjects’ rights, data operators’ obligations, and security measures [19].

Systemic Approach

The application of a systemic approach made it possible to consider national legal regulation as part of a broader system for personal data protection in international practice. Within this method, an analysis of the interrelations between various regulatory legal acts of Kazakhstan governing confidentiality and information protection in the healthcare sector was conducted.

Normative Approach

This method was applied to study and assess the effectiveness of existing national legal norms. It enabled the identification of compliance or non-compliance of Kazakhstan’s regulatory acts with international standards, as well as the detection of possible gaps and contradictions in legal regulation.

Content Analysis of Regulatory Legal Acts

A detailed content analysis of Kazakhstan’s existing laws and by-laws regulating personal data and medical information protection was conducted. Key documents were examined, including the Law of the Republic of Kazakhstan "On Personal Data and Their Protection," the Code "On People's Health and the Healthcare System," as well as subordinate acts regulating the processing, storage, and transfer of medical data.

Analysis of Judicial Practice

The study includes an analysis of court decisions regarding personal data protection and medical confidentiality in Kazakhstan. The main trends in law enforcement practices were identified, along with existing legal conflicts and gaps in the protection of patient data.

Thus, the application of these methods allowed for a comprehensive assessment of the level of legal protection of personal data in Kazakhstan, the identification of problematic aspects, and the proposal of ways to improve legislation in line with international standards.

ISSN 2524 – 0684 e-ISSN 2524 – 0692

Results

Sources of Medical Confidentiality in Kazakhstani Law

The foundation of legal regulation of relations related to the protection of the confidentiality of medical data is the Constitution of the Republic of Kazakhstan (1995, with subsequent amendments) [5]. In particular, Article 18 proclaims the inviolability of private life, while Article 19 establishes every person's right to the protection of their personal data. Although these provisions do not explicitly mention the term "medical confidentiality," their meaning implies the state's obligation to ensure the protection of any information affecting an individual's private sphere, including data on their health status [5].

The constitutional enshrinement of this right imposes responsibility on legislators and law enforcement agencies to develop and implement mechanisms that prevent unlawful access to medical information. Therefore, any restrictions or exceptions concerning confidentiality protection must be clearly regulated and comply with the principle of legality [20].

The key regulatory legal act explicitly establishing the institution of medical confidentiality in Kazakhstan is the Code "On People's Health and the Healthcare System" (hereinafter referred to as the Code), adopted in 2020 [8]. According to Article 95 of the Code:

"Healthcare professionals are required to maintain confidentiality regarding any information about a patient's health status, diagnosis, prognosis, treatment methods, and other data obtained during the provision of medical care."

This provision reflects the general principle of confidentiality and is further detailed in subsequent sections of the Code, which stipulate the requirement for the patient's mandatory consent before transferring relevant information to third parties. Additionally, the Code establishes that in cases of breach of medical confidentiality, the degree of legal liability—whether administrative or criminal—depends on the severity of the consequences and the harm caused to the patient [8].

Thus, the Code not only declares the obligation to maintain confidentiality but also establishes a direct link to legal protection mechanisms. This approach is intended to encourage healthcare professionals (and, in some cases, administrative personnel) to take a more responsible attitude toward storing and processing personal health data [21].

An important legal element that complements the overall framework of confidentiality is the Law of the Republic of Kazakhstan "On Personal Data and Their Protection" dated May 21, 2013, No. 94-V [9]. This law regulates the collection, processing, storage, and dissemination of any personal information, including biometric and other sensitive health data. The law stipulates that such data can only be processed with the subject’s consent or by direct legal mandate. In particular, Article 7 states that the collection and processing of personal data without consent are allowed only in cases explicitly provided for by law (for example, upon request from law enforcement agencies or in the event of a public health threat). This approach aims to minimize the risk of abuse by third parties and authorized state bodies [22, 23].

At the same time, there are several exceptions that allow bypassing the need for obtaining patient consent (Articles 8, 9, etc.) [9]. For example, when it comes to protecting the life and health of other individuals or conducting operational-search activities. These provisions, on the one hand, ensure a balance between protecting patient rights and safeguarding public interest, but on the other hand, they create prerequisites for a possible "erosion" of confidentiality if appropriate data access control procedures are not properly followed [24].

Special attention should be given to specific regulations that reflect the heightened sensitivity of certain categories of medical data [25]. For instance, Article 186 of the Code "On People's Health and the Healthcare System" explicitly regulates confidentiality issues in psychiatric care [8]. It emphasizes that information about a patient’s mental health, treatment methods, and related facts is subject to special protection. Similarly, the Law "On the

ISSN 2524 – 0684 e-ISSN 2524 – 0692

Prevention and Treatment of HIV Infection and AIDS" contains provisions aimed at protecting individuals with HIV-positive status from discrimination and unauthorized disclosure of information about their health condition [26].

Enhanced confidentiality measures in these cases are dictated by the high risks of stigmatization and potential discrimination against patients [27]. Despite this, practice shows that these guarantees may weaken under the influence of various regulations that allow government authorities (e.g., law enforcement agencies or sanitary-epidemiological services) to request relevant information in a number of exceptional situations [28]. In the absence of clear procedural rules, this could lead to uncontrolled expansion of the range of entities gaining access to particularly sensitive information [29].

Thus, Kazakhstan's legislation has established a multi-level legal mechanism that, on the one hand, enshrines the principle of medical secrecy and protects the patient from unlawful intrusion into their personal sphere, but on the other hand, includes exceptions that often allow bypassing the need for patient consent. How exactly these exceptions are implemented in practice and what factors contribute to the "erosion" of confidentiality will be the subject of further analysis.

Exceptions to Medical Confidentiality

Even with the formal recognition of the special status of medical confidentiality, the legislation of the Republic of Kazakhstan provides for cases where confidentiality protection may be limited by more significant (from the state's perspective) interests. In particular, Article 96 of the Code "On People's Health and the Healthcare System" establishes that the disclosure of medical information about a patient is possible in situations where there is a direct legal requirement [8]. If maintaining confidentiality contradicts specific legislative acts—such as the Criminal Procedure Code (CPC) of the Republic of Kazakhstan. According to Article 113 of the CPC, during a criminal investigation, pre-trial investigation authorities or the court may request necessary information, including medical documents.

Additionally, authorized bodies such as courts, prosecutors, investigative, and inquiry agencies have the right to request information covered by medical confidentiality when it is necessary for solving crimes or protecting public interests and national security (Article 96 of the Code and relevant articles of the CPC) [8,9].

The threat to the life and health of third parties should also be noted [30]. If there is a justified risk of an epidemic outbreak, the spread of a disease dangerous to others, or violent actions against other people, state authorities may require the disclosure of confidential information (Article 96 of the Code; similar provisions are found in certain regulatory acts of the Ministry of Health) [8,11].

Accordingly, just like patient consent itself, when a patient provides written consent, they have the right to determine which specific information and to what extent may be transferred to particular individuals or organizations. This principle aligns with the provisions of the Law "On Personal Data and Their Protection" (Article 8), which emphasizes the importance of the data subject's will [9].

Thus, these grounds demonstrate a balance between the protection of citizens' private lives and the necessity of safeguarding public interests. However, in real practice, there is not always a clear mechanism for notifying the patient that their medical data has been transferred to a particular agency. This may lead to a lack of transparency in the process and the absence of patient control over how and to whom information about their health is transmitted. The absence of such procedures increases the risk of unlawful or disproportionate interference in personal life, which, in the long run, could undermine public trust in the healthcare system [31].

Potential Threats to Medical Confidentiality in Kazakhstan

ISSN 2524 – 0684 e-ISSN 2524 – 0692

With the rapid development of digital technologies and their integration into the healthcare sector, Kazakhstan is forming state electronic databases of patients, electronic medical records, and other medical information systems (MIS). Additionally, eGov services are being implemented, allowing citizens to receive and transmit information remotely. Despite the obvious advantages (simplification of bureaucratic procedures, increased accessibility of medical services, and optimization of document management), these processes come with a number of risks.

For example, in addition to medical professionals, IT specialists and administrative personnel often have access to electronic databases. The regulation of their authority is not always clearly defined, which in turn increases the likelihood of unauthorized viewing or copying of confidential information, especially in the absence of strict access audits [32].

It is also important to consider hacker attacks, data leaks caused by unscrupulous employees, or an insufficient level of cybersecurity, which can lead to the loss or disclosure of patients' medical information. A unified medical data registry (for instance, within the framework of integration with eGov portals) may become an attractive target for cybercriminals.

The current legislation regulating the electronic processing and storage of medical data [8] is, in some cases, insufficiently coordinated. There are gaps and overlapping requirements, leading to practical difficulties and the risk of uncontrolled access to personal information.

In the digital age, the need for strict regulation and continuous improvement of cybersecurity measures is becoming one of the key priorities for preserving medical confidentiality [33].

Another important topic for discussion is the awareness of Kazakhstani citizens. A significant portion of the population of the Republic of Kazakhstan lacks sufficient knowledge about their rights and the mechanisms for protecting confidential medical information. For example, formal signing of consent for the processing of personal data or situations where patients often sign standard forms without reading their content and without understanding what exactly they are agreeing to.

These shortcomings indicate a lack of clarification from medical professionals. Healthcare personnel do not always provide detailed explanations of the legal consequences of sharing information with third parties. Patients are often unaware of which governmental or non-governmental organizations request their personal data from medical institutions and for what purpose.

As a result, the actual protection of patients' rights is weakened—even when formal confidentiality regulations exist, a citizen may find themselves faced with the fact of a data leak or transfer without knowing how and by what means to challenge such actions [34].

The Criminal Code of Kazakhstan mandates the compulsory notification of law enforcement authorities about certain serious crimes, particularly if there is a threat to the life and health of third parties [10]. A doctor who possesses information about such a crime may encounter a conflict between their professional duty to maintain patient confidentiality and their legally established obligation to notify the competent authorities.

However, the legislation and comments on the Criminal Code do not always provide clear criteria on when a doctor must override medical confidentiality in favor of public interest or the interests of justice. If a healthcare worker fails to report a planned or committed serious crime, they may face liability for concealment. At the same time, exceeding their authority and disclosing medical confidentiality without sufficient grounds entails other legal sanctions [10].

This legal contradiction poses a risk for healthcare professionals who, in trying to comply with the requirements of the Criminal Code, may inadvertently violate a patient's right to confidentiality.

ISSN 2524 – 0684 e-ISSN 2524 – 0692

Another concerning aspect is the broad and sometimes vague interpretation of terms such as "national security" or "public interest". Not all requests related to "state interests" require judicial approval or subsequent notification of the patient. The lack of mandatory judicial review (or oversight by another independent body) increases the risk of abuse. Furthermore, agencies with the authority to obtain data sometimes request more information than is necessary to address a specific issue, which poses a risk of violating citizens' privacy rights [9].

Thus, an expanded interpretation of "state necessity" may lead to unjustified intrusions into patients' personal lives, creating systemic prerequisites for limiting medical confidentiality and weakening constitutional protections.

Discussion. The structure and content of Kazakhstan's legislation demonstrate the state's commitment to ensuring a high level of confidentiality protection for medical data. The Constitution of the Republic of Kazakhstan (Articles 18, 19) establishes the fundamental provisions that serve as the basis for all subsequent regulatory acts in the field of medical confidentiality protection [5]. Additionally, the Code "On Public Health and the Healthcare System" (2020) and the Law "On Personal Data and Their Protection" (2013) define specific mechanisms for ensuring confidentiality and liability for its violation [9]. However, a detailed analysis of law enforcement practice reveals that several issues and contradictions reduce the real effectiveness of these norms.

Firstly, the extensive list of exceptions (Article 96 of the Code and corresponding provisions of the Criminal Procedure Code of the Republic of Kazakhstan) often leads to situations where the disclosure of medical information is permitted not only for the protection of genuine public interests (e.g., preventing serious crimes) but also under less critical circumstances [10]. This creates grounds for subjective interpretation of the norms and the risk of unjustifiably broad access by various agencies to patients' health information.

Secondly, the digitalization of healthcare and the development of electronic platforms (including public services on the eGov portal and medical information systems) require clearer regulatory frameworks. Researchers note that the existing bylaws lack clearly defined criteria for access rights differentiation and audit procedures in medical institutions. As a result, IT specialists, technical service staff, or government agencies may gain access to significant amounts of sensitive data without always understanding the limits of their authority. This increases the vulnerability of confidential information to cyberattacks and internal data leaks within healthcare institutions [35].

Thirdly, limited patient awareness of their rights and the responsibilities of medical professionals often leads to situations where individuals are unaware of which entities and on what grounds may receive information about their health. As a result, even lawful actions by law enforcement agencies or social services are perceived by patients as arbitrary and uncontrolled interference in their private lives. On the other hand, the absence of a notification mechanism for patients regarding the transfer of their data (except in rare cases) effectively deprives them of the ability to challenge potential abuses and protect their rights through judicial or administrative means [36].

Fourthly, a legal conflict often arises between a physician's duty to maintain medical confidentiality and the requirements of criminal law to report planned or committed crimes (Article 113 of the Criminal Procedure Code of the Republic of Kazakhstan and related provisions). A medical professional may find themselves in a situation where it is unclear which obligation should take precedence: protecting the patient as the holder of confidential information or serving the public interest in preventing criminal activity. The absence of uniform law enforcement guidelines increases the risk of a binary approach: either the doctor breaches confidentiality or risks being held accountable for concealing information [10].

ISSN 2524 – 0684 e-ISSN 2524 – 0692

Summarizing the above, it can be concluded that the legal framework generally reflects the principles of confidentiality; however, the implementation of these principles is complicated by numerous exceptions and insufficiently clear procedural control rules. In the context of increasing digitalization of healthcare, these gaps may become even more pronounced. To prevent a systemic decline in patient trust toward healthcare institutions, it is necessary to improve both the laws themselves and the mechanisms for their enforcement.

Proposals for Reforming Medical Confidentiality Legislation

The issue of medical confidentiality protection in the Republic of Kazakhstan requires comprehensive reform to ensure a balance between a patient's right to the inviolability of medical data and the needs of law enforcement agencies.

First and foremost, it is proposed to amend Article 273 of the Code of the Republic of Kazakhstan "On Public Health and the Healthcare System" [8]. Specifically, it is necessary to either eliminate the list of exceptions allowing the disclosure of medical confidentiality or clearly define the conditions for their application. It should be established that the provision of information at the request of investigative, prosecutorial, or judicial authorities is only permissible based on a court order or a prosecutor's decision with mandatory justification. This measure will ensure proper judicial oversight of access to medical data, preventing abuses and unjustified requests [37].

dditionally, it is proposed to develop an appropriate procedure in the Criminal Procedure Code of the Republic of Kazakhstan. The procedural framework for obtaining permission to access information constituting medical confidentiality should be clearly defined. Similar to the process for authorizing interrogations, an investigator should be required to apply to a court or an authorizing prosecutor with a reasoned petition justifying the necessity of obtaining specific medical data. The judge should promptly review the petition and issue a decision granting or denying access, specifying the exact data to be disclosed. This approach will prevent arbitrary access and ensure the legality of interventions [38].

It is also necessary to eliminate terminological ambiguity in Article 273 of the Code. Specifically, the concept of "harm to health caused by unlawful actions" should be detailed, clarifying that medical professionals inform the relevant authorities only in cases where there is a reasonable suspicion of a crime (e.g., gunshot wounds, assault) [8]. At the same time, the volume of disclosed information should be strictly limited: only the diagnosis and nature of the injury should be reported. Similarly, provisions regarding the transfer of information related to mental disorders and tendencies toward sexual violence should be clarified, requiring a preliminary conclusion from a medical commission and notifying guardianship authorities in cases of socially dangerous patient behavior [8].

Additionally, it is proposed to implement the principle of minimal disclosure of data. A rule should be established stating that even when there is a legal basis for disclosing medical confidentiality, the provided information must be limited to the necessary minimum. This principle aligns with international practice and aims to prevent excessive collection of personal data [39].

Finally, it is necessary to establish a mandatory registry of requests for the disclosure of medical information. Medical organizations must keep records of all requests, including the requesting authority, the volume of data provided, and the basis for the transfer of information. A mechanism should be in place to notify the patient about the fact of a request for their medical data after the investigation is completed, provided that such notification does not harm the justice process. This measure will ensure additional transparency and prevent unjustified intrusions into citizens' private lives [40].

Strengthening Responsibility for Violations of Confidentiality

ISSN 2524 – 0684 e-ISSN 2524 – 0692

Enhancing accountability for breaches of medical confidentiality is necessary to prevent illegal disclosure of medical data and to protect patients' rights. To toughen legislation, it is proposed to expand criminal and administrative liability, introduce mandatory notification of confidentiality violations, and establish mechanisms for compensation for harm.

First, Article 321 of the Criminal Code of the Republic of Kazakhstan needs to be revised [10]. Liability for the disclosure of medical information should extend not only to medical workers but also to any individual who has obtained such data through official duties or by other means. This will eliminate cases of impunity for disclosure, such as by law enforcement agencies or government officials. Sanctions should be tightened: for intentional disclosure without severe consequences – a fine of up to 1,000 MCI or imprisonment for up to 1 year; if the disclosure led to serious consequences (e.g., defamation of the patient, suicide attempts) – a fine of up to 5,000 MCI or imprisonment for up to 5 years. Aggravating circumstances should include abuse of official position and personal gain.

Second, administrative liability should be established for organizations that fail to protect medical data [41]. The Code of Administrative Offenses of the Republic of Kazakhstan should include an article on violations of information protection regimes, prescribing significant fines: for officials – 200–500 MCI and for legal entities – stricter sanctions with progressively increasing fines for repeated violations. Similar measures are provided for under the GDPR, where administrative fines can reach up to 4% of a company's annual turnover.

The third area involves introducing a mandatory notification requirement for confidentiality breaches [42]. Legally, medical organizations and personal data operators must be required to inform authorized bodies (e.g., Ministry of digital development, innovations and aerospace industry of the Republic of Kazakhstan) of violations within 72 hours and notify affected patients within 7 days. This will enhance system transparency and enable timely protective measures.

Additionally, the right of patients to claim moral damages in cases of unlawful disclosure of their medical data should be legally defined [43]. Explanations from the Supreme Court Plenum could specify the procedure for determining compensation, considering the degree of suffering caused. Special attention should be given to cases involving the disclosure of diagnoses that could lead to discrimination (e.g., HIV or mental illnesses) [44].

Moreover, patients should have the right to obtain information about the lawful disclosure of their data. Medical organizations must provide patients with details about who received their personal data and on what grounds after confidentiality restrictions are lifted (e.g., by court decision). This aligns with the principles of transparency and personal data control [44].

Cybersecurity Standards for Medical Data: Audit and Resilience Systems

Ensuring the security of medical data requires strict compliance with information security standards and regular oversight of their implementation [45]. To prevent data leaks and unauthorized access, the following measures are proposed:

First, regular security audits should be institutionalized [46]. Organizations processing medical data should be legally required to conduct independent information security audits at least once a year. The audit should include a compliance check of systems with security requirements, risk analysis, and penetration testing. The results should be documented in a report identifying vulnerabilities and recommending their remediation. This audit could become a mandatory condition for renewing a medical organization’s license or accreditation.

Second, state control and certification of medical information systems (MIS) should be introduced. Creating a registry of certified MIS that meet security requirements will help prevent the implementation of unprotected systems. Certification should be conducted at the level of an authorized body (e.g., Ministry of digital development, innovations and aerospace

ISSN 2524 – 0684 e-ISSN 2524 – 0692

industry of the Republic of Kazakhstan) in cooperation with cybersecurity centers. A similar approach is applied in the banking sector, where data protection standards are strictly regulated.

The third area involves specifying the minimum security requirements for MIS. Mandatory provisions should include annual system testing by third-party licensed organizations, the implementation of two-factor authentication, differentiation of access levels (administrator and super-administrator), and encryption of data both at rest and in transit.

Additionally, the principles of "privacy by design" and "security by design" should be adopted. The development of new electronic healthcare services must incorporate privacy and security requirements from the outset. For example, when creating patient applications, it is crucial to minimize unnecessary data collection and ensure protective mechanisms. This approach aligns with international standards, including the GDPR.

Another key measure is mandatory monitoring and incident response. Large medical resources must implement intrusion detection and logging systems and develop incident response plans outlining actions in case of breaches, system isolation, and digital forensics.

Furthermore, the qualification of technical personnel should be improved. The human factor is one of the key causes of data leaks [47]. Establishing mandatory training requirements for security administrators and conducting regular refresher courses will reduce the likelihood of phishing attacks and weak password use. Medical organizations should either employ an in-house information security specialist or contract an external company for security support.

Regular audits and penetration tests will help identify and address vulnerabilities before malicious actors exploit them. Strict security requirements will significantly complicate unauthorized access to data. In the era of digital healthcare, cybersecurity becomes an integral part of medical confidentiality. Implementing the proposed measures will ensure robust protection of patient personal data and increase trust in medical information systems.

Educational Measures and Means for Healthcare Workers and Patients

Raising awareness among all participants in medical relations about medical confidentiality and personal data protection plays a key role in ensuring privacy [48]. Legislative norms will be effective only if they are fully understood and realized by all parties involved.

First, it is necessary to introduce mandatory training and certification for healthcare workers on confidentiality issues [49]. All healthcare system employees—doctors, medical staff, pharmacists, and administrators—must undergo annual briefings or continuing education courses that include legal aspects of medical confidentiality and technical data protection skills (use of information systems, password protection, phishing detection). Upon completion of the training, an assessment should be conducted, similar to HIPAA requirements [50].

Second, the topic of medical confidentiality should be incorporated into the curricula of medical universities and colleges. Students must study the legal and ethical foundations of confidentiality, as well as cybersecurity issues in the medical field. In professional development programs for doctors, the study of information security should be mandatory.

The third direction is informing patients about their rights. During their first visit to a medical institution, patients should receive an informational leaflet explaining the privacy policy, the list of processed data, the purposes of its use, the individuals who have access, and the procedure for filing complaints in case of rights violations.

Signing informed consent for medical intervention should be accompanied by familiarization with the privacy policy [51].

Additionally, a system for informing patients about access to their data should be implemented. For example, patients could receive notifications (via SMS or electronically) when their medical record is accessed by a specific doctor.

ISSN 2524 – 0684 e-ISSN 2524 – 0692

Awareness efforts and methodological recommendations also play an important role. The Ministry of Health, together with authorized bodies, should develop and distribute guidelines for medical organizations describing procedures for ensuring confidentiality compliance, response algorithms for law enforcement requests, actions in case of suspected data leaks, internal investigations, and staff training. Moreover, informational campaigns should be conducted, including media publications, seminars for healthcare institution leaders, and the distribution of informational materials in clinics.

Furthermore, encouraging conscientiousness in data protection should be considered. The introduction of industry ratings or awards for a high level of confidentiality and the absence of data leaks will create positive motivation for medical organizations, making data protection not just an obligation but a reputational advantage.

Healthcare professionals should recognize not only the legal responsibility but also the moral aspect of protecting patient data. In turn, patients, knowing their rights, will be able to trust the healthcare system and provide complete information about their health without concerns about confidentiality. Awareness and education serve as sustainable mechanisms for protecting personal data and medical confidentiality [52].

Conclusion. The proposed reforms comprehensively strengthen the institution of medical confidentiality in Kazakhstan. The introduction of judicial oversight for access to medical data guarantees the protection of the constitutional right to privacy, raising the level of personal data security to international standards. Strengthening liability—both individual (criminal) and institutional (administrative)—creates effective sanction mechanisms and prevents violations. The introduction of mandatory patient notifications about instances of medical data disclosure enhances the fairness and reliability of the system.

Technical security standards and regular audits minimize the risks of data leaks, making medicine more secure in the era of digital transformation. This aligns with best practices under GDPR and HIPAA, ensuring a comprehensive approach to personal data protection. Awareness and training for medical professionals, administrative staff, and patients strengthen legal consciousness and foster a culture of confidentiality.

Importantly, the proposed reforms are based on international experience, adapting effective GDPR and HIPAA mechanisms to Kazakhstan's realities. For example, financial penalties will be proportionate to the national economic scale, and data access procedures will become more transparent and controlled. International enforcement practices (such as CNIL fines in France and record HIPAA settlements in the U.S.) demonstrate that such measures reduce the scale of violations and ensure their prompt detection and elimination.

The implementation of these changes will require legislative adjustments, the development of regulatory acts, staff training, and IT infrastructure modernization. However, these investments are justified, as increasing public trust in the healthcare system fosters more open interactions with doctors, improves patient adherence to treatment, and ultimately enhances the quality of medical care. Medical institutions, by avoiding data leaks, will preserve their reputation and prevent financial losses. The state, in turn, will fulfill its obligations to protect citizens' rights, demonstrating commitment to modern data security standards.

In an era where information has become a strategic resource, protecting confidentiality is a top priority. Medical confidentiality is not an archaic concept but a key tool for safeguarding citizens' dignity and privacy. A comprehensive reform based on the proposed measures will elevate Kazakhstan's legal framework to a new level, ensuring its compliance with global best practices. In the future, these principles may also be adapted for other sectors, such as education and social protection, which also handle significant amounts of personal data. The key is the consistent and conscientious implementation of these measures.

ISSN 2524 – 0684 **e-ISSN 2524 – 0692**

As a result, medical confidentiality in Kazakhstan will become truly inviolable, as required by law, medical ethics, and societal expectations.

Conflict of interest
We declare no conflict of interest**.**
Authors' contribution
Development of the concept, processing of results, interpretation of the results, writing the article- Iksatova S.T., Bekbatyrov B.Sh. Authors declare that this material has not been previously published and is not under consideration by other publishers.
Funding: None.

REFERENCES

1. Rieder P., Louis-Courvoisier M., Huber P. The end of medical confidentiality? Patients, physicians and the state in history // Medical Humanities. – 2016. – Vol. 42. – P. 149–154.
2. Han T., Gong X., Feng F., Zhang J., Sun Z., Zhang Y. Privacy-Preserving Multi-Source Domain Adaptation for Medical Data // IEEE Journal of Biomedical and Health Informatics. – 2023. – Vol. 27, No. 2. – P. 842–853. – DOI: 10.1109/JBHI.2022.3175071.
3. Uherek P. On medical confidentiality (not only) in time of coronavirus // Casopis lekaru ceskych. – 2020. – Vol. 159, No. 2. – P. 78–80.
4. Opgenhaffen T., de Koning M.B. Strikt persoonlijk? Het beroepsgeheim in tijden van gegevensbescherming // Tijdschrift voor Psychiatrie. – 2024. – Vol. 66, No. 8. – P. 421–425.
5. Конституция Республики Казахстан. – 1995. – URL: https://adilet.zan.kz/rus/docs/K950001000_/links (дата обращения: 15.03.2025).
   Konstitucija Respubliki Kazahstan. – 1995. – URL: https://adilet.zan.kz/rus/docs/K950001000_/links (data obrashhenija: 15.03.2025).
6. Фарбер Э. В. Врачебная тайна или медицинская тайна? // Медицинское право: теория и практика. – 2017. – Т. 3, № 2. – С. 139–144.
   Farber Je. V. Vrachebnaja tajna ili medicinskaja tajna? // Medicinskoe pravo: teorija i praktika. – 2017. – T. 3, № 2. – S. 139–144.
7. Бурмейстер И. А. Медицинская (врачебная) тайна: теоретический аспект // Сибирский юридический вестник. – 2008. – № 2. – С. 15–20.
   Burmejster I. A. Medicinskaja (vrachebnaja) tajna: teoreticheskij aspekt // Sibirskij juridicheskij vestnik. – 2008. – № 2. – S. 15–20.
8. Кодекс Республики Казахстан от 7 июля 2020 г. № 360-VI ЗРК «О здоровье народа и системе здравоохранения». – URL: https://adilet.zan.kz/ (дата обращения: 15.03.2025).
   Kodeks Respubliki Kazahstan ot 7 ijulja 2020 g. № 360-VI ZRK «O zdorov'e naroda i sisteme zdravoohranenija». – URL: https://adilet.zan.kz/ (data obrashhenija: 15.03.2025).
9. Закон Республики Казахстан от 21 мая 2013 г. № 94-V «О персональных данных и их защите». – URL: https://adilet.zan.kz/ (дата обращения: 15.03.2025).
   Zakon Respubliki Kazahstan ot 21 maja 2013 g. № 94-V «O personal'nyh dannyh i ih zashhite». – URL: https://adilet.zan.kz/ (data obrashhenija: 15.03.2025).
10. Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V ЗРК. – URL: https://adilet.zan.kz/ (дата обращения: 15.03.2025).

ISSN 2524 – 0684 e-ISSN 2524 – 0692

Ugolovnyj kodeks Respubliki Kazahstan ot 3 ijulja 2014 g. № 226-V ZRK. – URL: https://adilet.zan.kz/ (data obrashhenija: 15.03.2025).

11. Приказ Министра здравоохранения Республики Казахстан от 10 декабря 2020 г. № ҚР ДСМ-244/2020 «Об утверждении правил ведения первичной медицинской документации и представления отчетности». – URL: https://adilet.zan.kz/ (дата обращения: 15.03.2025).
Prikaz Ministra zdravoohranenija Respubliki Kazahstan ot 10 dekabrja 2020 g. № ҚR DSM-244/2020 «Ob utverzhdenii pravil vedenija pervichnoj medicinskoj dokumentacii i predstavlenija otchetnosti». – URL: https://adilet.zan.kz/ (data obrashhenija: 15.03.2025).
12. Приказ Министра здравоохранения Республики Казахстан от 24 июля 2024 г. № 58 «Об утверждении Правил обязательного страхования профессиональной ответственности медицинских работников». – URL: https://adilet.zan.kz/rus/docs/V2400034803 (дата обращения: 15.03.2025).
Prikaz Ministra zdravoohranenija Respubliki Kazahstan ot 24 ijulja 2024 g. № 58 «Ob utverzhdenii Pravil objazatel'nogo strahovanija professional'noj otvetstvennosti medicinskih rabotnikov». – URL: https://adilet.zan.kz/rus/docs/V2400034803 (data obrashhenija: 15.03.2025).
13. Mykhailichenko T.O., Horpyniuk O.P., Rak V.Yu. Medical confidentiality disclosure in conditions of epidemic threats // Wiadomosci Lekarskie. – 2021. – Vol. 74, No. 11 cz.2. – P. 2877–2883.
14. Комитет государственных услуг Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. Электронное правительство. – URL: https://www.gov.kz/memleket/entities/kgu/activities/1363?lang=ru (дата обращения: 15.03.2025).
Komitet gosudarstvennyh uslug Ministerstva cifrovogo razvitija, innovacij i ajerokosmicheskoj promyshlennosti Respubliki Kazahstan. Jelektronnoe pravitel'stvo. – URL: https://www.gov.kz/memleket/entities/kgu/activities/1363?lang=ru (data obrashhenija: 15.03.2025).
15. Wu Z., Xuan S., Xie J., Lin C., Lu C. How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective // Computers in Biology and Medicine. – 2022. – Vol. 147. – Article 105726. – DOI: 10.1016/j.compbiomed.2022.105726.
16. Bani Issa W., Al Akour I., Ibrahim A., et al. Privacy, confidentiality, security and patient safety concerns about electronic health records // International Nursing Review. – 2020. – Vol. 67, No. 2. – P. 218–230. – DOI: 10.1111/inr.12585.
17. Hu G., Li P., Yuan C., et al. Information Disclosure During the COVID-19 Epidemic in China: City-Level Observational Study // Journal of Medical Internet Research. – 2020. – Vol. 22, No. 8. – Article e19572. – DOI: 10.2196/19572.
18. Jeyaraman M., Ramasubramanian S., Kumar S., et al. Multifaceted Role of Social Media in Healthcare: Opportunities, Challenges, and the Need for Quality Control // Cureus. – 2023. – Vol. 15, No. 5. – Article e39111. – DOI: 10.7759/cureus.39111.
19. Jeyaraman N., Ramasubramanian S., Yadav S., et al. Regulatory Challenges and Frameworks for Fog Computing in Healthcare // Cureus. – 2024. – Vol. 16, No. 8. – Article e66779. – DOI: 10.7759/cureus.66779.
20. Sun W., Zhou Y., Chen W.T., et al. Disclosure experience among COVID-19-confirmed patients in China: A qualitative study // Journal of Clinical Nursing. – 2021. – Vol. 30, No. 5–6. – P. 783–792. – DOI: 10.1111/jocn.15616.

ISSN 2524 – 0684 e-ISSN 2524 – 0692

21. Daniel C., Kalra D. Clinical Research Informatics // Yearbook of Medical Informatics. – 2020. – Vol. 29, No. 1. – P. 203–207. – DOI: 10.1055/s-0040-1702007.
22. Yao Y., Yang F. Overcoming personal information protection challenges involving real-world data to support public health efforts in China // Frontiers in Public Health. – 2023. – Vol. 11. – Article 1265050. – DOI: 10.3389/fpubh.2023.1265050.
23. Thapa C., Camtepe S. Precision health data: Requirements, challenges and existing techniques for data security and privacy // Computers in Biology and Medicine. – 2021. – Vol. 129. – Article 104130. – DOI: 10.1016/j.compbiomed.2020.104130.
24. Torabi F., Orton C., Squires E., et al. Common governance model: a way to avoid data segregation between existing trusted research environment // International Journal of Population Data Science. – 2023. – Vol. 8, No. 4. – Article 2164. – DOI: 10.23889/ijpds.v8i4.2164.
25. Carnes N.A., Carey J.W., Gelaude D.J., et al. Improving HIV medical care engagement by attending to status disclosure and social support // AIDS Care. – 2021. – Vol. 33, No. 1. – P. 63–69. – DOI: 10.1080/09540121.2020.1718588.
26. Закон Республики Казахстан от 5 октября 1994 г. «О профилактике и лечении ВИЧ-инфекции и СПИДа». – URL: https://adilet.zan.kz/rus/docs/Z940006000 (дата обращения: 15.03.2025).
Zakon Respubliki Kazahstan ot 5 oktjabrja 1994 g. «O profilaktike i lechenii VICh-infekcii i SPIDa». – URL: https://adilet.zan.kz/rus/docs/Z940006000 (data obrashhenija: 15.03.2025).
27. Schweitzer A.M., Dišković A., Krongauz V., et al. Addressing HIV stigma in healthcare, community, and legislative settings in Central and Eastern Europe // AIDS Research and Therapy. – 2023. – Vol. 20, No. 1. – Article 87. – DOI: 10.1186/s12981-023-00585-1.
28. Reeves J.M., Zigah E.Y., Shamrock O.W., et al. Investigating the impact of stigma, accessibility and confidentiality on STI/STD/HIV self-testing among college students in the USA: protocol for a scoping review // BMJ Open. – 2023. – Vol. 13, No. 2. – Article e069574. – DOI: 10.1136/bmjopen-2022-069574.
29. Rivera A.S., Hernandez R., Mag-Usara R., et al. Implementation outcomes of HIV self-testing in low- and middle-income countries: A scoping review // PLoS One. – 2021. – Vol. 16, No. 5. – Article e0250434. – DOI: 10.1371/journal.pone.0250434.
30. Lally K. Disclosure // Journal of Palliative Medicine. – 2022. – Vol. 25, No. 6. – P. 1002–1003. – DOI: 10.1089/jpm.2022.0085.
31. Jia W., Jiao K., Ma J., et al. HIV infection disclosure, treatment self-efficacy and quality of life in HIV-infected MSM receiving antiretroviral therapy // BMC Infectious Diseases. – 2022. – Vol. 22, No. 1. – Article 937. – DOI: 10.1186/s12879-022-07932-z.
32. Tariq R.A., Hackert P.B. Patient Confidentiality // In: StatPearls [Internet]. – Treasure Island (FL): StatPearls Publishing, 2025 Jan–. – URL: https://www.ncbi.nlm.nih.gov/books/NBK519545/ (дата обращения: 15.03.2025).
33. Ostherr K. Artificial Intelligence and Medical Humanities // Journal of Medical Humanities. – 2022. – Vol. 43, No. 2. – P. 211–232. – DOI: 10.1007/s10912-020-09636-4.
34. DePuccio M.J., Di Tosto G., Walker D.M., McAlearney A.S. Patients' Perceptions About Medical Record Privacy and Security: Implications for Withholding of Information During the COVID-19 Pandemic // Journal of General Internal Medicine. – 2020. – Vol. 35, No. 10. – P. 3122–3125. – DOI: 10.1007/s11606-020-05998-6.

ISSN 2524 – 0684 e-ISSN 2524 – 0692

35. Inglada Galiana L., Corral Gudino L., Miramontes González P. Ethics and artificial intelligence // Revista Clínica Española. – 2024. – Vol. 224, No. 3. – P. 178–186. – DOI: 10.1016/j.rceng.2024.02.003.
36. Avci E. Protecting Incapacitated Patients' Rights and Best Interests // Indian Journal of Palliative Care. – 2023. – Vol. 29, No. 4. – P. 343–347. – DOI: 10.25259/IJPC_173_2022.
37. Clayton E.W., Embí P.J., Malin B.A. Dobbs and the future of health data privacy for patients and healthcare organizations // Journal of the American Medical Informatics Association. – 2022. – Vol. 30, No. 1. – P. 155–160. – DOI: 10.1093/jamia/ocac155.
38. Hoffman S. Privacy and Security – Protecting Patients' Health Information // New England Journal of Medicine. – 2022. – Vol. 387, No. 21. – P. 1913–1916. – DOI: 10.1056/NEJMp2201676.
39. Guo S.J., Chen H.C., Yen C.F. Estimation method for distance cost to access medical services: Policy and patient privacy implications in Taiwan // Frontiers in Public Health. – 2022. – Vol. 10. – Article 1065742. – DOI: 10.3389/fpubh.2022.1065742.
40. Wu G., Wang S., Ning Z., Zhu B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System // IEEE Journal of Biomedical and Health Informatics. – 2022. – Vol. 26, No. 5. – P. 1917–1927. – DOI: 10.1109/JBHI.2021.3123643.
41. Havers K.C.P. Breach of medical confidentiality // Medicine, Science and the Law. – 2025. – Vol. 93, No. 1. – P. 14–21. – DOI: 10.1177/00258172241274444.
42. Kroes S.K., Janssen M.P., Groenwold R.H., van Leeuwen M. Evaluating privacy of individuals in medical data // Health Informatics Journal. – 2021. – Vol. 27, No. 2. – Article 1460458220983398. – DOI: 10.1177/1460458220983398.
43. Williamson V., Murphy D., Stevelink S.A.M., et al. Confidentiality and psychological treatment of moral injury: the elephant in the room // BMJ Military Health. – 2021. – Vol. 167, No. 6. – P. 451–453. – DOI: 10.1136/bmjmilitary-2020-001534.
44. Raimundo G.C., Grando L.L., Machado A.N.C., et al. Ethical and bioethical aspects concerning the disclosure of medical information for a fair reason // Revista da Associação Médica Brasileira. – 2022. – Vol. 68, No. 2. – P. 202–205. – DOI: 10.1590/1806-9282.20211043.
45. Takahashi T., Zhihao Y., Omote K. Emergency Medical Access Control System Based on Public Blockchain // Journal of Medical Systems. – 2024. – Vol. 48, No. 1. – Article 90. – DOI: 10.1007/s10916-024-02102-x.
46. Gupta D.S., Mazumdar N., Nag A., Singh J.P. Secure data authentication and access control protocol for industrial healthcare system // Journal of Ambient Intelligence and Humanized Computing. – 2023. – Vol. 14, No. 5. – P. 4853–4864. – DOI: 10.1007/s12652-022-04370-2.
47. Jiang D., Shi G. Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare // Journal of Healthcare Engineering. – 2021. – Article 6656204. – DOI: 10.1155/2021/6656204. – Retraction: J Healthc Eng. – 2023. – Article 9850693. – DOI: 10.1155/2023/9850693.
48. Parobek C.M., Thorsen M.M., Has P., et al. Video education about genetic privacy and patient perspectives about sharing prenatal genetic data: a randomized trial // American Journal of Obstetrics and Gynecology. – 2022. – Vol. 227, No. 1. – P. 87.e1–87.e13. – DOI: 10.1016/j.ajog.2022.03.047.
49. Basil N.N., Ambe S., Ekhator C., Fonkem E. Health Records Database and Inherent Security Concerns: A Review of the Literature // Cureus. – 2022. – Vol. 14, No. 10. – Article e30168. – DOI: 10.7759/cureus.30168.

ISSN 2524 – 0684 e-ISSN 2524 – 0692

50. Baric-Parker J., Anderson E.E. Patient Data-Sharing for AI: Ethical Challenges, Catholic Solutions // Linacre Quarterly. – 2020. – Vol. 87, No. 4. – P. 471–481. – DOI: 10.1177/0024363920922690.
51. Pietrzykowski T., Smilowska K. The reality of informed consent: empirical studies on patient comprehension-systematic review // Trials. – 2021. – Vol. 22, No. 1. – Article 57. – DOI: 10.1186/s13063-020-04969-w.
52. Varkey B. Principles of Clinical Ethics and Their Application to Practice // Medical Principles and Practice. – 2021. – Vol. 30, No. 1. – P. 17–28. – DOI: 10.1159/000509119.

Авторлар туралы мәліметтер

@Иксатова С.Т., з.ғ.д.,профессор, Инновациялық Еуразия университеті, iksatovast@gmail.com, https://orcid.org/ https://orcid.org/ 0009-0000-4683-9707 .

Бекбатыров Б.Ш., магистрант, Инновациялық Еуразия университеті, bakhtiyar.sh@gmail.com, https://orcid.org/ https:// 0009-0007-7312-0563 .

Information about authors

@Iksatova S.T., Doctor of Law, Professor, Innovative University of Eurasia, iksatovast@gmail.com, https://orcid.org/ 0009-0000-4683-9707 .

Bekbatyrov B.Sh., Master's student, Innovative University of Eurasia, bakhtiyar.sh@gmail.com, https://orcid.org/ https://orcid.org/ 0009-0007-7312-0563.

Сведения об авторах

@Иксатова С.Т., д.ю.н.,профессор, Инновационный Евразийский университет, iksatovast@gmail.com, https://orcid.org/ 0009-0000-4683-9707 .

Бекбатыров Б.Ш., магистрант, Инновационный Евразийский университет, bakhtiyar.sh@gmail.com, https://orcid.org/ https://orcid.org/ 0009-0007-7312-0563 .

ҚАЗАҚСТАННЫҢ ҚҰҚЫҚТЫҚ ЖҮЙЕСІНДЕГІ ДӘРІГЕРЛІК ҚҰПИЯ: НАҚТЫ ЖЕКЕ ӨМІРДІ ҚОРҒАУ ҚҰРАЛЫ МА?

С.Т. ИКСАТОВА, Б.Ш. БЕКБАТЫРОВ

Инновациялық Еуразия университеті, Павлодар, Қазақстан

Түйіндеме

Кіріспе. Дәрігерлік құпия – пациенттің жеке деректерін қорғаудың және жеке өмірге қол сұғылмаушылық құқығын қамтамасыз етудің маңызды элементтерінің бірі. Қазақстанда денсаулық сақтау жүйесінің цифрлануы және мемлекеттік органдардың өкілеттіктерінің кеңеюі аясында медициналық мәліметтердің құпиялылығын сақтау мәселесіне қатысты жаңа сын-қатерлер туындауда.

Мақсаты. Бұл мақала Қазақстан Республикасында дәрігерлік құпия институтының құқықтық реттелуін талдау, заңнамалық олқылықтар мен медициналық деректердің құпиялылығына төнетін қауіптерді анықтау, сондай-ақ құқық қолдану тәжірибесін жетілдіру бойынша ұсыныстар әзірлеуге бағытталған.

Материалдар мен әдістер. Зерттеуде салыстырмалы-құқықтық талдау, жүйелі және нормативтік әдістер қолданылып, қолданыстағы нормалардың халықаралық стандарттарға (GDPR, HIPAA) сәйкестігі бағаланды. Сонымен қатар, Қазақстан

ISSN 2524 – 0684 e-ISSN 2524 – 0692

Республикасының нормативтік-құқықтық актілеріне және сот практикасына контент-талдау жүргізілді.

Нәтижелер. Қазақстан заңнамасы дәрігерлік құпияны формалды түрде қорғауды қамтамасыз етеді, алайда пациенттің келісімінсіз мемлекеттік органдарға медициналық деректерді сұратуға мүмкіндік беретін бірқатар ерекшеліктер де бар. Негізгі мәселелердің қатарына ұлттық қауіпсіздік критерийлерінің нақтыланбауы, цифрлық медициналық деректер базасына қолжетімділіктің жеткіліксіз реттелуі және пациенттерге олардың деректерінің үшінші тұлғаларға берілуі туралы хабарламаудың тиімді тетіктерінің жоқтығы жатады. Сондай-ақ, медициналық ақпараттық жүйелердің киберқауіпсіздік деңгейінің төмендігі және пациенттердің өз құқықтары туралы жеткіліксіз хабардар болуы ақпараттың сыртқа таралу қаупін арттыратыны анықталды.

Қорытынды. Қазақстанда медициналық құпияны қорғау деңгейін арттыру үшін бірнеше бағыттар бойынша реформалар қажет: медициналық деректерді жария ету туралы сұрау салуларға сот бақылауын күшейту, оларды заңсыз таратқаны үшін қылмыстық және әкімшілік жауапкершілікті күшейту, ашықтық пен пациенттерді хабардар ету тетіктерін енгізу, киберқауіпсіздік стандарттарын жетілдіру. Медициналық қызметкерлерге арналған білім беру бағдарламаларын әзірлеу және пациенттердің құқықтық сауаттылығын арттыру да медициналық құпияны сақтау институтын нығайту және оны цифрлық дәуірге бейімдеу жолындағы маңызды қадамдар болып табылады.

Түйінді сөздер: дәрігерлік құпия, жеке деректер, құпиялылық, киберқауіпсіздік, жеке өмірге қол сұғылмаушылық құқығы, Қазақстан, денсаулық сақтаудың цифрлануы, медициналық ақпарат, құқықтық реттеу

ВРАЧЕБНАЯ ТАЙНА В ПРАВОВОЙ СИСТЕМЕ КАЗАХСТАНА: РЕАЛЬНЫЙ ЛИ ЭТО ИНСТРУМЕНТ ЗАЩИТЫ ЧАСТНОЙ ЖИЗНИ ПАЦИЕНТА?

С.Т. ИКСАТОВА, Б.Ш. БЕКБАТЫРОВ

Инновационный Евразийский университет, Павлодар, Казахстан

Аннотация

Введение: Врачебная тайна представляет собой один из ключевых элементов защиты персональных данных пациента и обеспечения права на неприкосновенность частной жизни. В условиях цифровизации здравоохранения и расширения полномочий государственных органов в Казахстане возникают новые вызовы, связанные с соблюдением конфиденциальности медицинских сведений.

Цель. Данная статья направлена на анализ правового регулирования института врачебной тайны в Республике Казахстан, выявление существующих законодательных пробелов и угроз для конфиденциальности медицинских данных, а также разработку предложений по совершенствованию правоприменительной практики.

Методы. В исследовании применены методы сравнительно-правового анализа, системного и нормативного подходов, позволяющие оценить соответствие действующих норм международным стандартам (GDPR, HIPAA). Также использован контент-анализ нормативно-правовых актов Казахстана и судебной практики.

Результаты. Установлено, что законодательство Казахстана формально обеспечивает защиту врачебной тайны, однако содержит ряд исключений, позволяющих государственным органам запрашивать персональные медицинские данные без согласия

ISSN 2524 – 0684 **e-ISSN 2524 – 0692**

пациента. Существенные проблемы связаны с размытостью критериев национальной безопасности, недостаточной регламентацией доступа к цифровым медицинским базам, а также отсутствием эффективных механизмов контроля и уведомления пациентов о передаче их данных третьим лицам. Выявлены риски утечек информации в связи с недостаточным уровнем кибербезопасности медицинских информационных систем и низкой осведомленностью пациентов о своих правах.

Заключение. Для повышения уровня защиты врачебной тайны в Казахстане необходимы реформы в нескольких направлениях: усиление судебного контроля при запросах на раскрытие медицинских данных, ужесточение уголовной и административной ответственности за их незаконное распространение, внедрение механизмов прозрачности и уведомления пациентов, а также совершенствование стандартов кибербезопасности. Развитие образовательных программ для медицинского персонала и повышение правовой грамотности пациентов также являются важными шагами к усилению института врачебной тайны и его адаптации к цифровой эпохе.

Ключевые слова: врачебная тайна, персональные данные, конфиденциальность, кибербезопасность, право на частную жизнь, Казахстан, цифровизация здравоохранения, медицинская информация, правовое регулирование