JOURNAL OF INTELLECTUAL PROPERTY AND HUMAN RIGHTS

Volume: 3 Issue: 10 | Oct–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

The Legal Aspects of Organizing Personal Data in Healthcare

Yusupova Faringiz Uktam qizi, Ph.D
Teacher of the "International Law and Human Rights" Department of Tashkent state university of law

Abstract: Since the introduction of information and telecommunications technologies into the healthcare sector, there has been an increasing demand for medical services and the development of healthcare systems. This scientific work focuses on the legal aspects of ensuring the security of personal data in the healthcare system, particularly concerning the protection of patients' medical information. The research analyzes national and international legal norms related to personal data protection, revealing their specific applications within the healthcare system. Additionally, it addresses pressing issues of confidentiality and information security in the handling of medical data. The article also discusses the obligations of organizations and professionals in the healthcare sector regarding the storage of patients' personal data and their responsibilities to protect against illegal use. Furthermore, it explores the interconnection between international legal practices and national legislation concerning the security of personal data in healthcare, as well as modern methods of protecting personal information in the context of digital technology development. The study concludes with proposals aimed at enhancing the security of personal data within the healthcare system.

Keywords: Personal data security, healthcare law, data protection, medical confidentiality, legal norms, data security legislation, medical data security, information security, protection of confidential information, electronic healthcare, personal data legislation, digital security, international legal standards, healthcare system, illegal use of data.

Introduction

Improving the quality of medical services provided to the population worldwide, along with the digitization of healthcare and the effective use of telemedicine technologies, is one of the goals of sustainable development. Numerous scientific articles and research projects are prioritized in this area. In this context, analyzing the normative activities of the World Health Organization as a specialized institution involved in international regulation of medical assistance quality is essential. This includes monitoring the implementation of normative-legal documents governing bilateral cooperation, reviewing legislative norms based on the requirements of ratified conventions, ensuring the safety of personal data utilized through telemedicine technologies, and strengthening the implementation of international standards into national legislation.

In the foreign policy strategy of the Republic of Uzbekistan with prestigious international organizations, measures are being taken to strengthen and further develop mutually beneficial cooperation, as well as to enhance the implementation of the norms of ratified international treaties concerning fundamental rights in the field of healthcare law into national legislation. In this context, the President of the Republic of Uzbekistan, Sh.M. Mirziyoyev, has emphasized that "it is impossible to modernize and renew our country without the broad development of information and communication technologies and the Internet" [1]. Indeed, "providing quality medical services to the population through the use of information and telecommunication technologies, establishing a modern system, implementing these technologies in family polyclinics and rural health posts for primary healthcare, creating a unified centralized telemedicine system under the Republican Specialized Scientific-Practical Center, and improving the electronic healthcare network based on advanced information technologies" are defined as national tasks for sustainable development. From this perspective, it is of urgent importance to develop proposals and recommendations aimed at further

Volume: 3 Issue: 10 | Oct–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

enhancing the legal foundations of mutually beneficial international cooperation with the World Health Organization, which plays a leading role in regulating healthcare law at the international level.

In this context, not only have many international documents been adopted by international organizations, but also by our Republic. These include the World Health Organization's "Global Health Sector Digitalization" Strategy for 2020-2025, the World Health Assembly's resolution WHA58.28 on electronic health, the WHO's eHealth Resolution (2005), the European Parliament and Council's Directive 2011/24/EU on "Patients' Rights in Cross-Border Healthcare," the Republic of Uzbekistan's Law on "Citizen Health Protection" (1996), the Presidential Decree of the Republic of Uzbekistan dated January 28, 2022, PF-60 on the "Development Strategy of New Uzbekistan for 2022-2026," the Concept for the Development of the Health Sector of Uzbekistan for 2019-2025, the decision dated October 20, 2018, No. 841 on "Effective Organization of Digitalization in the Health Sector," and the decisions on "Measures for Implementing National Goals and Objectives in the Field of Sustainable Development until 2030," among other legal documents. The successful implementation of the tasks outlined in these documents will be significantly supported by this dissertation research.

When studying the creation of databases for digitization in the healthcare sector and ensuring their confidentiality, it is essential to analyze the structures of the authorized institution responsible for processing incoming data by dividing them into two main areas.

The first area includes collecting information and its initial processing, obtaining consent from patients for data processing, and handling data related to the staff of the medical institution. The second area involves payroll management by human resources and accounting, where salaries are determined based on individual performance indicators, as well as the salaries paid for remote medical services[2].

It is also important to note that, in addition to personal data, medical institutions possess non-personal data, which is utilized for writing scientific articles and collecting statistical information.

By identifying the regulatory and legal framework that governs the confidentiality of data in medical institutions, we can explore the shortcomings and issues within this field.

In the Republic of Uzbekistan, the primary regulatory and legal document aimed at regulating this area is the Law on "Personal Data." This law outlines the procedures for processing and protecting personal data and applies to relationships arising from the use of processing means, including information technologies.

Furthermore, the law provides a definition of personal data, which refers to information related to a specific individual or that can identify an individual, recorded in electronic form, on paper, or in other tangible forms.

Ensuring the security of personal data in the healthcare sector is a pressing issue, and various scholars are proposing different approaches to this topic. According to E. Usmanova and K. Gorbacheva, "personal data" refers to any information that can be used to identify an individual. This includes the person's name, address, date of birth, and other personal information.[3]

O. Gostin, a renowned expert in health law, emphasizes that protecting personal data within the healthcare system is essential for strengthening the legal foundations of the health system. He particularly highlights the necessity of developing and implementing international and national legislative norms for the protection of personal data in healthcare. According to Gostin, improving the legislation on personal data protection in healthcare should rely on international experiences[4].

Linda T. conducted research on the protection of personal data within the healthcare system in the United Kingdom. She pays special attention to the issue of using patient data without their consent. According to her, every patient should be aware of how their medical information is used and who has

Volume: 3 Issue: 10 | Oct–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

access to it. She proposes further strengthening the legislation to ensure the confidentiality of medical data within the UK healthcare system [5].

David Gunkel, a prominent scholar in information technology and information security, conducts in-depth research on medical technologies and the security of personal data. He believes that modern technologies, particularly artificial intelligence and data analytics, require the development of innovative solutions for the protection of personal information. Gunkel also emphasizes the need to maintain a balance between technical and legal measures in the development of information security policies in healthcare. [6]

Based on the views of foreign scholars, the legal aspects of protecting personal data in the healthcare sector are related to improving national legislation, developing it in line with international standards, and taking modern technologies into account. At the same time, there needs to be a delicate balance between supporting innovations in legislation and protecting patients' personal rights.

In our opinion, the confidentiality of medical data emphasizes the importance of strengthening legal norms related to information and monitoring them on a legal basis, including the collaboration between law enforcement agencies and representatives of the healthcare system. At the same time, it highlights the necessity of developing mechanisms for monitoring personal data in the healthcare system through information technologies.

Materials and Methods

In addressing the topic, methods such as historical analysis, systematic legal analysis, comparison, and comparative-legal analysis have been utilized.

Research Results

Ensuring the security of personal data in the healthcare sector is currently one of the important issues. With the advancement of modern medicine, electronic health systems and digital health services are widely employed. This necessitates addressing the collection, storage, and utilization of patients' personal and medical data. The illegal use of patients' personal information and breaches of information security can negatively affect the reliability of the healthcare system. Therefore, in recent years, various countries have been conducting research to ensure the security of personal data in the healthcare sector.[7].

The security of medical data refers to the protection of personal and confidential medical information from unauthorized access, breaches, and disclosure. This issue has become increasingly pressing with the development of modern technologies. Scholars and experts express various opinions on the security of medical data. Below are some common viewpoints:

According to Jonsen AR and Winslade WJ, the necessity to protect medical data is very high because it is personal and confidential. If the data falls into the wrong hands, it can have negative consequences during the provision of medical services, including the potential harm to patients' health or leading to incorrect treatments[8].

According to Rubin E.B., it is suggested to enhance digital protection tools for the security of medical data. For example, methods such as strengthening protection through cryptography, utilizing artificial intelligence for security measures, and monitoring data through blockchain technologies are considered crucial [9].

The increasing number of cyberattacks on healthcare systems is raising concerns among researchers. Since medical data holds significant value, it can be stolen or used for extortion. Therefore, scholars recommend strengthening cybersecurity measures in healthcare institutions.

Volume: 3 Issue: 10 | Oct–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Overall, researchers and professionals in the medical field view the issue of medical data security as a pressing problem that requires the integration of technological advancements, legal standards, and cybersecurity measures.

The General Data Protection Regulation (GDPR), which came into force in 2018 by the European Union, marked an important milestone in protecting personal data in the healthcare sector. Researchers have studied the impact of this legal document on the healthcare system. Studies indicate that GDPR ensures strict oversight in the collection, storage, and use of personal data in healthcare settings. For instance, research conducted by Anne Wesley and Mark Taylor has positively assessed the role of GDPR in ensuring personal data security in healthcare and emphasized its reinforcement of principles such as obtaining patient consent and limiting the use of personal data.[10].

Due to the widespread use of electronic health systems and Electronic Health Records (EHR), researchers are deeply analyzing issues related to information security. In her research on the security of electronic health records, Moskovkina E.K. recommends measures such as data encryption, restricting access rights, implementing security protocols, and training staff in information security. She also emphasizes the necessity of using consent-based approaches in processing medical data and strengthening privacy policies. [11].

Sog‘liqni saqlash tizimida bemorlarning shaxsiy ma’lumotlari bilan ishlash jarayonida bemorning roziligi muhim ahamiyatga ega. **David J. Gunkel** o‘z tadqiqotlarida, bemorlarning roziligini olish jarayonida raqamli texnologiyalar qo‘llanilishi kerakligini ta’kidlaydi[12]. Uning tadqiqotlari bemorning roziligini elektron shaklda olish, rozilik jarayonini soddalashtirish va ularni oson kuzatish imkoniyatini yaratish orqali shaxsiy ma’lumotlarning noqonuniy ishlatilishining oldini olish mumkinligini ko‘rsatadi. Bundan tashqari, shaxsiy ma’lumotlardan qanday foydalanilayotgani to‘g‘risida bemorlarga to‘liq ma’lumot berish tizimning ochiqligini oshiradi va ishonchni mustahkamlaydi.

In recent years, research on ensuring the security of personal data during the use of artificial intelligence (AI) and big data analytics in the healthcare system has been increasing. John W. Ladley and Cathy O'Neil have studied the security aspects of processing personal data in healthcare systems based on AI and recommend developing innovative methods to ensure data security through AI technologies. Their research indicates that it is essential to enhance technologies that maintain the anonymity and security of personal data during the processes of data analysis and forecasting using AI[13].

Encryption technologies are considered one of the primary methods for protecting personal data in the healthcare system. Leading experts in information security, such as Bruce Schneier, have conducted research on ensuring the confidentiality of medical records through encryption. Their studies show that applying strong encryption algorithms during the transmission and storage of medical data enhances security and helps prevent data breaches. Additionally, Paul Syverson focuses on developing systems that detect alterations to medical data or unauthorized access.[14].

Significant research is being conducted in the United States and European countries to ensure the security of personal data in the healthcare sector. Abedjan and Ziawasch studied the impact of the GDPR legislation in the European Union on healthcare systems and analyzed the Health Insurance Portability and Accountability Act (HIPAA) regulations in the United States. Their research indicates that leveraging international experiences is an effective method for ensuring data security in national healthcare systems. In particular, implementing global standards for the use and protection of data in healthcare helps better safeguard patients' rights[15].

Volume: 3 Issue: 10 | Oct–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Analysis of Research Results

The issue of protecting personal data in the healthcare sector should be addressed not only through technical and legal measures but also by studying international experiences and integrating them into national legislation. Research conducted on ensuring the security of personal data in healthcare has shown that the combined application of technical and legal measures plays a significant role in safeguarding data. The need to enhance security measures in electronic health systems, including technologies for protecting personal data, encrypting medical records, and analyzing big data with artificial intelligence, is increasingly growing. Additionally, by studying international practices and legal standards and adapting them to national systems, the security of personal data in the healthcare sector can be further strengthened.

Conclusions

The healthcare system in the Republic of Uzbekistan is consistently developing, making the protection of personal data, particularly medical records, a pressing issue. Medical data includes information about a patient's health, treatment history, medical examination results, and other personal details. If misused or disseminated, such information can violate the rights of the patient. Therefore, a series of legal measures must be implemented to ensure the security of personal data in the healthcare sector of Uzbekistan.

The law on "Personal Data," adopted on July 2, 2019, has established an important legal foundation for data protection. This law clearly defines the procedures for collecting, storing, processing, and transmitting personal data. However, due to the specific nature of healthcare data, there is a need to develop special regulations to ensure their confidentiality. Additionally, there is a demand for supplementary rules to prevent the illegal processing and use of personal data in the healthcare sector.

Uzbekistan's healthcare system is undergoing a transition to electronic formats. This process requires extensive use of information technologies within the healthcare system. The implementation of Electronic Health Records (EHR) simplifies the medical service delivery process, but it also necessitates enhanced measures to ensure the security of personal data. The following actions can be taken to achieve this goal:

1. **Data Encryption**: It is essential to apply strong encryption technologies during the transmission and storage of personal patient data in electronic systems. This will help protect the data from unauthorized access and misuse.
2. **Access Control**: Access to medical data should be restricted to designated professionals only. Those with access rights must adhere to confidentiality policies, and ongoing monitoring should be established.
3. **Strengthening Information Security Protocols**: Regular security audits should be conducted in healthcare systems, along with strict measures to protect against malware and to create data backups.

REFERENCES

1. Sh.Mirziyoyev.-Sog’liqni saqlash tizimini zamon talabi darajasida takomillashtirish –kun tartibidagi asosiy masala//Sh.Mirziyoyev Milliy taraqiyot yo’limizni qatiyat bilan davom etirib yangi bosqichga kutaramiz. – T.:“O’zbekisoton”.NMIU 2017, – B.309.
2. Rosique I, Pérez-Cárceles MD, Romero-Martín M, Osuna E, Luna A. The use and usefulness of information for patients undergoing anaesthe-sia. Med Law2006;25:715-27

Volume: 3 Issue: 10 | Oct–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

3. Usmanova E.F., Gorbacheva K. S. Kultura processualnix dokumentov // XLVII Ogavervskie chteniya: Materiali nauchnoy konferensii. Saransk: Nacionalniy issledovatelskiy Mordovskiy issledovatelskiy Mordovskiy gosudarstveniy universitet im. M.P.Ogavyova, 2019. S. 527-530
4. O.Gostin -Xalqaro sog'liqni saqlash huquqi kontseptsiyasining ibtidosi / N.V. Sajienko / Professor P. E. xotirasiga bag'ishlangan xalqaro huquq bo'yicha xalqaro o'qishlar. Kazanskiy: ota. uchinchi xalqaro konferensiya Sci. konf. (m. Odessa, 2-3 barg tushishi 2012 yil) / vdp. bitiruv uchun yuridik fanlar nomzodi, dotsent. M. I. Pashkovskiy; Milliy "Odeska yuridik akademiyasi" universiteti. - Odessa: Feniks, 2012. - P. 115-118.
5. Linda T. Kohn, Janet M. Corrigan, and Molla S. Donaldson, Editors; Committee on Quality of Health Care in America, Institute of Medicine
6. Health system efficiency. How to make measurement matter for policy and management. Copenhagen: WHO Regional Office for Europe, 2016.
7. Axborot tizimlarida shaxsiy ma'lumotlarni himoya qilish sog'liqni saqlash: sog'liqni saqlash sohasida qo'llaniladigan tamoyillar va tartiblar. Kopengagen: JSSTning Yevropa mintaqaviy byurosi; 2020. Litsenziya: CC BY-NC-SA 3.0 IGO
8. Jonsen AR, Siegler M, Winslade WJ. *Clinical Ethics: A Practical Approach to Ethical Decisions in Clinical Medicine*. 7th ed. New York, NY: McGraw Hill; 2010:174.
9. Rubin E.B. Professional conduct and misconduct. *Handbook of Clinical Neurology*. 2013;118:91-105.
10. Gillies MA, Baldwin FJ. Do patient information booklets increase peri-operative anxiety? Eur J Anaesthesiol 2001;18:620
11. Moskovkina E.K. Patient’s Privacy and Relatives’ Rights in Genetic Research.Lex Genetica. 2023;2(2):53-73. (In Russ.)
12. David J. Gunkel- The Machine Question: Critical Perspectives on AI, Robots, and Ethics
13. John. Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program. Waltham: Morgan Kaufmann, 2012. https://doi.org/10.1016/C2011-0- 04633-1 accessed 20.11.2021
14. Paul Syverson: Privacy-Protecting COVID-19 Exposure Notification Based on Cluster Events. CoRR abs/2201.00031(2022)
15. Abedjan, Ziawasch et al. “Data science in healthcare: Benefits, challenges and opportunities”. In: Data Science for Healthcare. Springer, 2019, pp. 3–38.