JOURNAL OF INTELLECTUAL PROPERTY AND HUMAN RIGHTS

Volume: 3 Issue: 8 | Aug–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Data Ownership and Control in the Context of Big Data Applications in Healthcare

Imamalieva Diyora Imamali kizi
Lecturer at the Department of International Private Law Tashkent State University of Law

Abstract: The exponential growth of big data in healthcare has led to unprecedented opportunities for improving patient outcomes, optimizing healthcare operations, and advancing medical research. However, this expansion also raises significant challenges concerning data ownership and control. This article explores the complex landscape of data ownership in the context of big data applications within healthcare, examining the legal, ethical, and practical implications for stakeholders, including patients, healthcare providers, and data custodians. The discussion delves into the evolving definitions of data ownership, the rights of individuals versus the rights of organizations, and the role of consent in data collection and utilization. Furthermore, the article addresses the tension between the need for data accessibility to foster innovation and the imperative to protect patient privacy and ensure data security. By analyzing current regulatory frameworks and emerging trends, the article provides insights into how data ownership and control are being negotiated and what this means for the future of big data in healthcare.

Keywords: big data, privacy, data ownership, ethical standards, personal data, cross-border transfer, healthcare system.

Introduction

Traditionally, ownership of health-related data has been attributed to the individuals who own the data. Individuals have a vested interest in controlling the use and disclosure of their personal health information, and this right is protected by privacy laws and regulations[1]. However, as healthcare systems increasingly collect and aggregate vast amounts of data, the issue of ownership has become increasingly complex.

Healthcare providers, researchers, and institutions also have legitimate interests in health-related data. Healthcare providers generate and collect data in the course of providing healthcare, and researchers seek access to such data to advance medical knowledge and improve treatment outcomes. In addition, private companies, such as technology companies and pharmaceutical companies, may have commercial interests in accessing and analyzing health-related data for product development and innovation.

The legal framework for data ownership and control varies across jurisdictions. In some countries, the default position is that individuals own their health data and control its use[2]. However, there are cases where individuals may willingly share their data for research purposes or to optimize treatment. In these cases, individuals may enter into data sharing agreements or consent to the use of data under certain conditions.

[1] 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[2] Mittelstadt, B. D., & Floridi, L. (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. Science and engineering ethics, 22(2), P. 318

Volume: 3 Issue: 8 | Aug–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

In addition to individual ownership, models of collective ownership and governance have been proposed to account for the complex nature of health-related data. Data cooperatives and data commons are examples of collaborative models in which participants collectively own and manage data, allowing for broader access for research and public health purposes[3]. These models aim to achieve a balance between privacy rights and the societal benefits that can result from data sharing and analysis.

Intellectual property rights also matter when considering data ownership and control. Ideas, discoveries and innovations generated by the analysis of health-related data may be subject to intellectual property protection, such as patents or copyrights. Balancing the interests of data owners, users and the general public is critical to ensuring that intellectual property rights do not hinder the broader benefits and advances that can be achieved through the use of big data in healthcare. It is essential to develop clear legal frameworks and governance structures that address data ownership and control. This includes defining the rights and responsibilities of data providers, establishing mechanisms for sharing and accessing data, and protecting privacy rights. Collaborative efforts involving policymakers, lawyers, healthcare providers and data providers are needed to develop comprehensive and fair solutions that promote data sharing for healthcare while respecting the rights and interests of individuals.

Research scope

Data ownership and control pose significant legal challenges in the context of big data and artificial intelligence in healthcare. This section examines the complex legal landscape surrounding data ownership, data access, and data control, considering the implications for individuals, healthcare providers, and researchers. The analysis includes relevant legal frameworks, research, and case law to provide a comprehensive understanding of the topic.

1. Data ownership. Data ownership refers to the legal rights and control over data. In the healthcare context, data ownership can be vested in a variety of stakeholders, including patients, healthcare providers, and researchers. However, defining data ownership in the big data and artificial intelligence space can be challenging due to the collaborative nature of data collection, sharing, and analysis. Legal frameworks and agreements should clearly address data ownership, ensuring that the rights of individuals are respected, and healthcare organizations and researchers should have clear guidelines on how to use and share data[4].
2. Data access and consent. Access to health data for research purposes must comply with legal requirements and ethical considerations. Informed consent plays a critical role in granting access to sensitive health data. Researchers must obtain appropriate consent from individuals for the collection, use and sharing of their data. Legal frameworks such as data protection regulations provide guidance on obtaining valid consent and ensuring individuals have control over their data. Clear and transparent consent processes should be established to address the complexities of data access and consent in the context of big data and artificial intelligence research[5].
3. Data control and governance. Data control includes the ability to manage and govern data throughout its lifecycle, including its storage, access and use. Effective data controls are essential to protect privacy, ensure data security, and prevent unauthorized use or disclosure. Legal frameworks and organizational policies should establish robust data governance frameworks that

[3] Rumbold, J. M., & Pierscionek, B. (2017). The Effect of the General Data Protection Regulation on Medical Research. Journal of medical Internet research, 19(2), P. 47
[4] Price, W. N., 2nd, & Cohen, I. G. (2019). Privacy in the age of medical big data. Nature medicine, 25(1), 37–43.
[5] 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Volume: 3 Issue: 8 | Aug–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

define the responsibilities and obligations of data custodians, researchers, and other relevant parties. These frameworks should include data protection measures, data sharing agreements, methods for anonymizing data, and mechanisms to address breaches or unauthorized access to data[6].

4. Intellectual Property Rights. Intellectual property (IP) rights may also intersect with data ownership in the context of big data and artificial intelligence in healthcare. AI algorithms, models, and discoveries derived from the analysis of health data may raise intellectual property issues. Legal frameworks related to patents, copyrights, and trade secrets provide protection for intellectual property generated by AI. It is essential to find a balance between IP rights and the public interest in advancing medical knowledge. Legal frameworks should provide clarity on the ownership and use of AI-generated intellectual property to encourage innovation and ensure equal access to advances in health.
5. International data transfer. Big data and artificial intelligence research often involves international collaboration and cross-border data sharing. Legal challenges arise when transferring medical data internationally due to different data protection laws and regulations. Adequate safeguards, such as data transfer agreements and adherence to internationally recognized standards, should be in place to ensure compliance with applicable rules and protect privacy rights. Harmonization efforts and international cooperation can facilitate data sharing while ensuring legal compliance and upholding ethical standards[7].

In the Republic of Uzbekistan, the integration of big data into healthcare gives rise to various legal complexities that need to be addressed to ensure responsible and ethical use of data.

First, the legal status of health-related data is important. The Decree of the President of the Republic of Uzbekistan dated May 25, 2021 No. 5124 “On additional measures for the integrated development of the healthcare sector” emphasizes the need to create conditions for increasing the capacity of health workers and proposes the development of regulations for the collection, storage and use of healthcare data. Defining the legal status of health-related data includes defining ownership rights, access privileges and consent requirements for their use in research, treatment and public health initiatives.

Second, legal issues arise when collecting big data. The Law of the Republic of Uzbekistan dated August 30, 2002 No. 402-II “On the donation of blood and its components” establishes rules for the collection and use of blood and its components. When it comes to collecting big data, ensuring compliance with the law when obtaining patient data, genetic information, or other health-related data from various sources can be challenging. Clear guidelines are needed to navigate the legal environment and ensure that data collection practices comply with existing laws and regulations.

Another area of concern is data ownership and control. The Law of the Republic of Uzbekistan dated May 24, 2023 No. 844 "On Restricting the Distribution and Consumption of Alcohol and Tobacco Products" addresses issues related to the protection of personal information and privacy. In the context of big data, it is critical to establish clear boundaries of ownership and control over health-related data, ensuring that individuals' privacy rights are respected and their data is properly protected.

Privacy and data protection also pose legal challenges. Current regulations, protection of personal information, and data security. These laws provide a framework to ensure that health-related data

[6] National Institute of Standards and Technology Cybersecurity Framework, URL: https://www.nist.gov/cyberframework, Date of access: 12.06.2024
[7] EU Standard Contractual Clauses, URL: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, Date of access: 09.06.2024

Volume: 3 Issue: 8 | Aug–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

collected and processed in the context of big data analytics are protected from unauthorized access, hacking, or misuse.

To address these legal complexities, the Republic of Uzbekistan may further develop and implement a comprehensive legal framework specifically designed to handle big data in healthcare. This may include the creation of specific rules, guidelines and standards that provide clarity on data ownership, access, consent, privacy, security and international data transfers. In addition, regular updates and amendments to existing laws, as well as ongoing consultation and collaboration with relevant stakeholders, can help ensure that the legal framework keeps pace with the changing landscape of big data in healthcare.

Addressing legal issues related to data ownership, access, control, and intellectual property rights in the context of big data and artificial intelligence in healthcare requires comprehensive legal frameworks, clear policies, and collaborative efforts among stakeholders. It is essential to find a balance between protecting privacy rights, advancing scientific advances, and encouraging innovation. Legal frameworks must evolve to keep pace with technological advances and address emerging ethical and legal issues in this rapidly evolving field.

Based on an analysis of the relevant legal framework, research, and case law, it is clear that a robust legal framework should prioritize individual rights, establish transparent consent processes, define clear data governance mechanisms, and address intellectual property considerations. In addition, international cooperation and harmonization efforts should be aimed at ensuring consistency and compliance with legal standards when sharing data.

Thus, effective legal solutions to address data ownership, access, control, and intellectual property issues in the context of big data and artificial intelligence in healthcare require a multifaceted approach that takes into account individual rights, ethical considerations, and advances in technology. By implementing comprehensive legal frameworks and facilitating collaboration among stakeholders, legal complexities can be addressed and the potential benefits of big data and artificial intelligence in healthcare can be maximized.

LIST OF REFERENCES:

1. Закон Республики Узбекистан «О донорстве крови и ее компонентов» от 30.08.2002 г. № 402-II // *Национальная база данных законодательства, 22.11.2023 г., № 03/23/879/0873*
2. Закон Республики Узбекистан «Об ограничении распространения и употребления алкогольной и табачной продукции» 24.05.2023 г. № ЗРУ-844 // *Национальная база данных законодательства, 25.05.2023 г., № 03/23/844/0293*
3. Постановление Президента Республики Узбекистан «О дополнительных мерах по комплексному развитию сферы здравоохранения» от 25.05.2021 г. № ПП-5124 // *Национальная база данных законодательства, 16.06.2023 г., № 06/23/96/0379*
4. 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1. URL: https://eur-lex.europa.eu/eli/reg/2016/679/o
5. Mittelstadt, B. D., & Floridi, L. (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. Science and engineering ethics, 22(2), P. 318
6. Rumbold, J. M., & Pierscionek, B. (2017). The Effect of the General Data Protection Regulation on Medical Research. Journal of medical Internet research, 19(2), P. 47

Volume: 3 Issue: 8 | Aug–2024 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

7. Price, W. N., 2nd, & Cohen, I. G. (2019). Privacy in the age of medical big data. Nature medicine, 25(1), 37–43.
8. National Institute of Standards and Technology Cybersecurity Framework, URL: https://www.nist.gov/cyberframework, Date of access: 12.06.2024
9. EU Standard Contractual Clauses, URL: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, Date of access: 09.06.2024
10. Abujarad F, Alfano S, Bright TJ et al. Building an informed consent tool starting with the patient: The patient-centered virtual multimedia interactive informed consent (VIC). AMIA Annu Symp Proc. 2017;2017:374–383.
11. Carman D, Britten N. Confidentiality of medical records: the patient's perspective. Br J Gen Pract. 1995 Sep;45(398):485–8.
12. Имамалиева, Диёра Имамали Кизи (2024). ЮРИДИЧЕСКИЕ СЛОЖНОСТИ, СВЯЗАННЫЕ С ПРИМЕНЕНИЕМ БОЛЬШИХ МЕДИЦИНСКИХ ДАННЫХ. Oriental renaissance: Innovative, educational, natural and social sciences, 4 (2), 287-294.