



<https://doi.org/10.22363/2313-2337-2024-28-3-565-583>


EDN: HWMBJC

Research Article / Научная статья

Law and digitalization of modern healthcare

Olga V. Romanovskaya  , Georgy B. Romanovskiy 

Volgograd State University, *Volgograd, Russian Federation*

 pgu-gpd@yandex.ru

Abstract. The article addresses the issues in healthcare delivery and organization of public healthcare in the face of rapid advancements in digital technologies. The purpose of the study is to outline the legal challenges arising during the implementation of concepts such as digital health, e-health, mobile health as well as establishing the legal framework for electronic medical records and telemedicine, and certain types of innovative biomedical activities. The article illustrates the consistent impact of information and communication technologies on the interaction between patients and healthcare providers. It defines the legal framework for telemedicine and its transition to e-health. The study systematizes the particularities of legal regulations concerning both general electronic medical record and those developed by specialized medical organizations. It presents legal challenges related to data compatibility and potential cross-border exchanges. The concept of mobile healthcare is analyzed, with attention given to the risks associated with its development, notably threats to privacy and cybersecurity. The main directions of digital medicine and the challenges faced by modern legal regulations are summarized, including the use of big data, the integration of artificial intelligence, translational bioinformatics, gamification of various stages of medical care, etc. Additionally, the legal challenges arising from the use of big data and introduction of certain digital devices into medical practice are outlined, with special attention given to the brain-computer interface. Comprehensive recommendations for the improvement of healthcare legislation are presented.

Key words: legal regulation, e-health, mobile health, electronic health record, digital health, biomedicine, telemedicine

Conflict of interest. The authors declare no conflict of interest.

The authors' contribution: *Romanovskaya O.V.* – introduction, concept, scientific analysis of materials; *Romanovskiy G.B.* – scientific leadership, theoretical substantiation of the study, generalization of the results obtained, conclusion.

Funding. The study was financed by the grant of the Russian Science Foundation No. 24-28-00365, <https://rscf.ru/project/24-28-00365/>

Received: 18th January 2024

Accepted: 15th July 2024

© Romanovskaya O.V., Romanovskiy G.B., 2024



This work is licensed under a Creative Commons Attribution 4.0 International License
<https://creativecommons.org/licenses/by-nc/4.0/legalcode>


For citation:

Romanovskaya, O.V., Romanovskiy, G.B. (2024) Law and digitalization of modern healthcare. *RUDN Journal of Law*. 28 (3), 565–583. (in Russian). <https://doi.org/10.22363/2313-2337-2024-28-3-565-583>

Право и цифровизация современного здравоохранения

О.В. Романовская  , Г.Б. Романовский 

Пензенский государственный университет, г. Пенза, Российская Федерация

 pgu-gpd@yandex.ru

Аннотация. Раскрываются актуальные проблемы оказания медицинской помощи и организации общественного здравоохранения в условиях стремительного развития цифровых технологий. Цель исследования – охарактеризовать юридические проблемы, возникающие в процессе внедрения таких концепций, как цифровое здравоохранение, электронное здравоохранение, мобильное здравоохранение; определить правовой режим электронной медицинской карты и телемедицины, некоторых видов инновационной биомедицинской деятельности. Показано последовательное влияние информационно-коммуникационных технологий на процесс взаимодействия пациента и медицинского работника. Определен правовой режим телемедицины, а также ее переход к электронному здравоохранению. В статье систематизированы особенности правового регулирования как общей электронной медицинской карты, так и создаваемых специализированными медицинскими организациями. Представлены юридические проблемы совместимости данных, а также возможного трансграничного обмена. Проанализирована концепция мобильного здравоохранения. Уделено внимание рискам, возникающим в силу ее развития, где основное место занимают угрозы неприкосновенности частной жизни и кибербезопасности. Обобщены основные направления цифровой медицины и ее сложности, с которыми сталкивается современное правовое регулирование, а именно: использование больших данных и внедрение искусственного интеллекта, трансляционная биоинформатика и геймификация различных этапов оказания медицинской помощи и др. Обозначены правовые проблемы, возникающие при внедрении в медицинскую практику некоторых цифровых устройств, где особое внимание уделено интерфейсу «мозг-компьютер». Представлены комплексные рекомендации по совершенствованию здравоохранительного законодательства.

Ключевые слова: правовое регулирование, электронное здравоохранение, мобильное здравоохранение, электронная медицинская карта, цифровое здравоохранение, биомедицина, телемедицина

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Вклад авторов: Романовская О.В. – ведение, концепция, научный анализ материалов; Романовский Г.Б. – научное руководство, теоретическое обоснование исследования, обобщение полученных результатов, заключение.

Финансирование. Исследование выполнено при финансовой поддержке Российского научного фонда в рамках научного проекта № 24-28-00365, <https://rscf.ru/project/24-28-00365/>

Поступила в редакцию: 18 января 2024 г.

Принята к печати: 15 июля 2024 г.

Для цитирования:

Романовская О.В., Романовский Г.Б. Право и цифровизация современного здравоохранения // *RUDN Journal of Law*. 2024. Т. 28. № 3. С. 565–583. <https://doi.org/10.22363/2313-2337-2024-28-3-565-583>

Introduction

The rapid advancement of digital technologies has led to extensive transformations of the key aspects of human life. Information and communication technologies (ICT) that specify modern interpersonal communication are at the core of all interactions. As indicated in various regulatory documents, digitalization of healthcare is among the legal policy priorities of the Russian Federation. Therefore, the Presidential Council for Strategic Development and National Projects approved the Passport for the priority project of October 25, 2016, Protocol No. 9 On Improving the Processes of Organizing Medical Care Based on the Introduction of Information Technologies. Subsequently, the Passport for the Healthcare national project was supplemented by the federal project of December 24, 2018, Protocol No. 16 On Creation of a Unified Digital Circuit in Healthcare Based on the Unified State Health Information System (USHIS). The establishment of a unified digital circuit is among the key objectives of the Strategy for Healthcare Development in the Russian Federation until 2025, approved by the Presidential Decree of the Russian Federation No. 254 of June 06, 2019, and the Strategic Direction of Digital Transformation of Healthcare No. 3980-r, approved by the Government of the Russian Federation on December 29, 2021. Additionally, the Ministry of Health of the Russian Federation and the Federal Service for Supervision of Healthcare in the Russian Federation have approved various departmental digital transformation programs within the Digital Public Administration federal project of the Digital Economy of the Russian Federation national program.

Digital technologies play a significant role in establishing horizontal connections, providing real-time information and services, thereby accelerating social processes and opening up new avenues for the advancement of P4 medicine¹. In the Russian Federation, this holistic approach to healthcare is known as “personalized medicine”. The Concept of Predictive, Preventive and Personalized Medicine, endorsed by the Order of the Ministry of Health of Russia No. 186 of April 24, 2018, aims to enhance a patient-oriented healthcare. Therefore, digitalization can provide a technological foundation for personalized medicine.

The digital transformation also brings profound changes to the public health sector. Rapid and intelligent processing of large amounts of data enables better allocation of financial resources, aids in predicting public health promotion, disease prevention, and development of healthcare logistics. As data accumulates, it is crucial for the government to adhere to principles of transparency that underpin the concept of open data².

¹ An English term used to denote the four elements of a new paradigm in the healthcare panorama. Each “p” individuates *predictive*, *preventive*, *personalized*, and *participatory* medicine.

² The Ministry of Health of the Russian Federation: Open Data. Available at: <https://minzdrav.gov.ru/opendata> [Accessed 06th February 2024].

Legal aspects of electronic health and electronic medical record

The integration of computers into the healthcare system has rapidly led to process automation, and the development of healthcare informatics. Concurrently, the use of telecommunication technologies for transmitting information gave rise to the concept of telemedicine in the early 1990s. Various models for data transfer were explored, uncovering persistent challenges that remain relevant today: ensuring patient data protection (Margolis, 1994:14), maintaining the reliability of consultations (Sanders & Bashshur, 1995:118), and establishing clear responsibilities for all participants in the consultations (Brahams, 1995:199). Telemedicine, critical in current times, has dramatically expanded its potential through diverse methods of real-time data exchange. It acts as a digital aid in revolutionizing access to healthcare.

However, Russian legislation has struggled to keep pace with the advancements in telemedicine. The Concept for the Development of Telemedicine Technologies in the Russian Federation and its Implementation Plan were approved by the Ministry of Health and the Russian Academy of Medical Sciences on August 27, 2001, under Order No. 344/76. Despite this, tangible legal frameworks failed to gain support from the State Duma of the Federal Assembly of the Russian Federation. The Draft Federal Law No. 308883-4 On Information and Communication Technologies in Medicine was officially introduced by some deputies in 2006, but was not considered until its exclusion in 2011. This issue was brought to attention following the President's message in 2016, which promptly led to the adoption of the Federal Law No. 242-FZ of July 29, 2017 On Amendments to Certain Legislative Acts of the Russian Federation on Application of Information Technologies in the Sphere of Healthcare. Subsequently, the Procedure for Organizing and Providing Medical Care Using Telemedicine Technologies was approved by the Ministry of Health on November 30, 2017, under Order No. 965n.

The advancement of Information and Communication Technologies (ICT) has led to the concept of “electronic health” (e-health), introduced by John Mitchell who is widely credited with establishing this term, marking a transition from telemedicine. He defined e-health as a new term needed to describe “the combined use of electronic communication and information technology in the health sector for clinical, educational, research and administrative purposes, both at the local site and at a distance” (Mitchell, 1999:55). The term gained popularity, especially after Intel Corporation (Santa Clara, California, USA) described e-health as “a concerted effort undertaken by leaders in health care and hi-tech industries to fully harness the benefits available through convergence of the Internet and health care”. Gunther Eysenbach further elaborated on e-health as “an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology. As such, the “e” in e-health does not only

stand for “electronic”, but implies a number of other “e’s”, which together perhaps best characterize what e-health is all about”. The 10 e’s in “e-health” represents various aspects such as efficiency, quality enhancement, evidence based practices, empowerment, encouragement, education, information exchange facilitation, expanding healthcare reach, ethics, and equity (Eysenbach, 2001). While the definitions by J. Mitchell and G. Eysenbach are commonly used in encyclopedias and basic publications on e-health, there are still variations in understanding the concept.

Given holistic understanding of e-health and the conventional terminology, the lingering conceptual “discrepancy” distinguishes three major concepts:

- e-health as healthcare based on innovative technologies;
- e-health as a set of technological capabilities and infrastructure applied to deliver healthcare services;
- e-health as a service sector and component of the commercial sector (e-commerce) to maximize profits.

Given such perceptual diversity of the term, the legal approaches or, more accurately, the goals to be set in forming the legal framework would need to be adjusted. If the objective is healthcare regulation, then the focus should be on healthcare providers and patients; if the objective is technology, then the interests of hardware and software developers take precedence; if the objective is the market sector, then commercial interests are crucial. Apparently, the government should address all aspects, while ensuring the protection of patient-physician interests.

The implementation of an electronic medical record (EMR) is a key guideline for the development of e-health both in Russia and internationally. As for the Russian Federation, the EMR sparked significant debate while developing the Concept for the Development of the Healthcare System in the Russian Federation until 2020 in the 2010s. A.A. Mokhov was among the first legal scholars to interpret the EMR term as “a document that contains personal information about the patient, requests for medical assistance, services provided, therapy performed, invasive interventions, vaccinations administered, and other life characteristics (developmental anomalies, injuries sustained, allergic reactions, etc.)” (Mokhov, 2010:23).

While the electronic medical record (EMR) remains relevant, its adoption is not widespread in the country, except for the advanced model implemented in Moscow³. This platform is supplied with a remote server to systematize data (limited to Moscow) and a mobile app to track real-time information. In 2009, a unified portal of state and municipal services commonly referred to as Gosuslugi was established, featuring a Health profile component. This digital platform, operated by the Russian government, functions as a federal information system and is accessed through an informational block rather than a personalized specialized card. Users can input data into their personal profiles on this shared resource.

³ The Official Portal of the Moscow Mayor and Moscow Government: Your Electronic Medical Record. Available at: <https://www.mos.ru/city/projects/medcarta/?ysclid=lox8k640vz450123579> [Accessed 06th February 2024].

Legal development took place in 2017 when the innovation was launched with the Federal Law No. 242-FZ of July 29, 2017 (previously mentioned in connection with telemedicine). This was followed by the adoption of the Government of the Russian Federation's Order No. 2521-r of November 15, 2017, which approved the List of Healthcare Services that can be provided to citizens in electronic form through the unified portal of state and municipal services by the unified state information system in the field of healthcare.

The legal foundation for electronic medical records (EMR) can be found in the Federal Law No. 326-FZ of November 29, 2010, On Mandatory Medical Insurance in the Russian Federation, which provides funding for maintaining patient medical records in electronic form (Article 50, Part 3, Clause 2). Subsequently, the Ministry of Health of Russia approved the Main Sections of the Electronic Medical Record through its Order No. 18-1/1010 of November 11, 2013, in alignment with the aforementioned law. This framework specifies the EMR as “a set of electronic personal health records (ePHR) related to an individual patient to be collected, stored, and used within a single healthcare organization”. Despite allowing for the creation of multiple EMR for patients seeking help from various medical organizations, the current system lacks a mechanism for patients to provide feedback or make any alterations to their own records.

The Order of the Ministry of Health of Russia No. 834n of December 15, 2014, On Approval of Unified Forms of Medical Documentation Used in Medical Organizations Providing Outpatient Medical Care, included several documents, with the outpatient medical record (form No. 025/u) being one of them. The Order of the Ministry of Health of Russia No. 2n of January 09, 2018, On Amendments to the Order of the Ministry of Health of the Russian Federation No. 834n of December 15, 2014, specified that the outpatient medical record should be generated in electronic form (Clause 2.1). The Order of the Ministry of Health of Russia No. 947n of September 07, 2020, On Approval of the Procedure for Organizing a Document Management System in Health Protection in Regard to Maintaining Medical Documentation in the Form of Electronic Documents, came into force to regulate medical electronic document management. It should be noted that specialized medical organizations maintain their own patient medical records for various specialties such as oncology, phthisiology, psychiatry, psychiatry and narcology, dermatology, dentistry, and orthodontics. The long-term work plan of the Federal Fund for Mandatory Medical Insurance (FFMMI) for 2023⁴ featured the initiation of activities related to a digital patient profile to monitor the quality of medical care and ensure proper distribution of the FFMMI finances.

The Unified State Health Information System (USHIS) serves as a technological platform within the legal framework determined by the Governmental Decree No. 140 of February 09, 2022, On the Unified State Information System in the Field of Healthcare. The Unified State Health Information System (USHIS) is designed to encompass a wide range of medical data and administrative functions, including patient registers, dispensary registration certificates, medical care accounting catalogs, healthcare

⁴ Approved by the FFMMI Board on December 29, 2022 (Decision No. 1, Protocol No. 4).

organization and medical worker registers, statistical observation records and various analytical tables.

The system is also anticipated to facilitate the transfer of medical records (such as MRI and CT scans) and to serve as a platform for certain telemedicine functions. Additionally, the platform is expected to connect various *electronic healthcare* stakeholders, including patients, healthcare organizations, medical professionals, healthcare authorities, and players in the pharmaceutical market (both wholesale and retail), creating a comprehensive system for information exchange covering public and personal health aspects. The significant data volume of the USHIS must be forecasted to ensure effective management and utilization.

Despite the forward-looking nature of this “super service”, its current usage appears to be limited. Many aspects remain unregulated by law, hindering the accumulation and utilization of data. For instance, the legal framework for data management has not been fully established, as highlighted by the Federal Law No. 126-FZ of April 30, 2021, which outlined the registration of electronic sick leave certificates via the Gosuslugi platform with minimal patient involvement. It is evident that while certain activities, such as obtaining a sick leave certificate, can be completed through Gosuslugi, other interactions with non-governmental healthcare providers, involving the management of personal medical data, are not currently integrated into the platform. Furthermore, the regional expansion of Electronic Medical Records (EMR) by the constituent entities of the Russian Federation, along with the development of a regional portal for medical services, represents another technological advancement in the healthcare sector.

An analysis of the European practices has revealed that the adoption of special legislation governing electronic medical records (EMR) for patients is uncommon. One notable example is the Federal Act on Electronic Patient Records, which was implemented in Switzerland on June 19, 2015 and officially came into force on April 15, 2017⁵. According to Article 2 of this act, an electronic patient record (EPR) is described as a “virtual dossier that allows decentralized storage of treatment-relevant data from a patient’s medical history or their personal recorded data, which can be accessed during specific treatment cases”. In a session on June 28, 2023, the Federal Council proposed a corresponding revision of the Federal Act on the Electronic Patient Record for consultation. Under a proposed revision, a free EPR will be automatically created for all individuals residing in Switzerland with mandatory health or military insurance. Each individual will have the authority to determine which healthcare professionals have access to their EPR. Additionally, individuals who do not wish to have an EPR can submit an objection to prevent its creation. This opt-out model aims to promote wider dissemination and use of EPR, positioning them as a central component of the healthcare system. Moreover, the medical data stored in EPRs hold significant value for researchers. The proposed revision of the Act would also allow individuals with an EPR to explicitly consent to making non-anonymized medical data from their EPR available for research purposes. In order to access the EPR,

⁵ Die Publikationsplattform des Bundesrechts: Bundesgesetz über das Elektronische Patientendossier. Available at: <https://www.fedlex.admin.ch/eli/cc/2017/203/de> [Accessed 06th February 2024].

there are plans to introduce a future national electronic identification (e-ID) interoperable with digital certificates for citizens.

European Union (EU) member states operate under overarching regulations for personal data processing, with specific emphasis on the confidentiality and sensitivity of medical data. As such, Electronic Records (EPR) is subject to the General Data Protection Regulation (GDPR)⁶ within the EU member states. While the stringent restrictions enforced by the GDPR aim to safeguard privacy, they have faced criticism from healthcare professionals who argue that strict compliance impedes the collection of crucial data necessary for advancing public health initiatives. Evert-Ben van Veen has highlighted the incompatibility of social networking concepts with the secure management of medical record banks (Van Veen, 2018:70–80). Concerns have also been raised by academics, such as Williams (Williams, 2018:508) and Staunton, Slokenberga, and Mascalzoni (Staunton, Slokenberga & Mascalzoni, 2019), regarding GDPR requirements that could significantly impede medical data research.

In 2019, the European Commission adopted the Recommendation on a European Electronic Health Record Exchange Format⁷ to facilitate the interconnectivity of Electronic Health Records (EHR) across EU borders. This initiative aims to assist EU countries in their efforts to ensure that citizens can securely access and exchange their health data throughout the EU. Despite the advancements made and the allocation of financial resources, there are persistent challenges that hinder the seamless integration of unified information systems, exemplified by the regulatory obstacles between Finland and Estonia⁸.

The widespread EHR adoption offers numerous benefits, but its successful implementation and acceptance hinge on effectively mitigating the associated privacy and security risks (Kierkegaard, 2011). Some scholars highlight the retention of bulk data as an example of modern state surveillance (Birrer, He & Just, 2023). Given the sensitive nature of health data, individuals consulting healthcare professionals inherently expect a level of confidentiality that originally emerged as a social construct to foster trust in medical practitioners. However, with the current level of digitalization, the concept of confidentiality has evolved into more technocratic forms of data protection, akin to a ‘zombie category’ that persists its changing meaning (Wadmann, Hartlev & Hoeyer, 2023).

The global trend towards universalization is facilitated by the adoption of the unified standard set by the International Organization for Standardization (ISO), specifically ISO

⁶ 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). Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed 06th February 2024].

⁷ The Official Website of the European Union: Recommendation on a European Electronic Health Record Exchange Format (C(2019)800) of February 6, 2019. Available at: <https://digital-strategy.ec.europa.eu/en/library/recommendation-european-electronic-health-record-exchange-format> [Accessed 06th February 2024].

⁸ The Official Website of the European Union: eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the EU. Lot 1 – Interoperability of Electronic Health Records in the EU (Final Report, 2020). Available at: <https://digital-strategy.ec.europa.eu/en/library/interoperability-electronic-health-records-eu> [Accessed 06th February 2024].

10781:2023 Health Informatics – HL7 Electronic Health Record-System Functional Model, Release 2.1 (EHR FM)⁹. While the pursuit of universality requires significant technological efforts rather than jurisprudential considerations, several key features warrant attention:

- Technical regulations often take precedence over legal norms in various domains.
- Interaction models and data transfer protocols may differ, and adopting a unified approach may not always align with such constitutional values such as security and confidentiality.
- Achieving e-health objectives depends on technological independence, as lacking proprietary technological solutions may lead to dependence on foreign entities within a country's population.
- The development of technological capabilities must be coupled with the cultivation of specialized skills and competencies among healthcare professionals and patients to effectively leverage modern digital opportunities.

When designing the national legal framework for the EMR, it is essential to consider each of the aforementioned aspects.

Legal aspects of mobile health

The advancement of multi-purpose mobile phones (smartphones) and messaging platforms for real-time information exchange has transformed the fundamentals of interpersonal communication, consequently affecting healthcare. This shift has been amplified by the proliferation of diverse gadgets that enable individuals to independently monitor personal health metrics, gather health data, and access a range of personalized assistance. An array of portable tech devices is now available from pharmaceutical companies, including tonometers, glucometers, pulse oximeters, multi-function cholesterol meters, blood uric acid meters, and drug delivery systems. Additionally, portable and wearable ultrasonic system-on-patch (USoP) devices have been developed for applications like early-stage breast cancer detection (Burgess, Gluskin & Pinker, 2023:1948) and monitoring deep tissues in moving subjects (Lin, Zhang & Gao, et al., 2023), etc.

Smart watches, a modern accessory widely used in everyday life, offer functionalities such as tracking the number of steps taken, monitoring cardiovascular fitness and blood oxygen levels, measuring heart rate, heart rhythm, body temperature, and blood pressure. There are publications highlighting the use of smart watches for diagnosing cardiovascular conditions and preventing myocardial infarctions (Drexler et al, 2020:2224).

The advancement of such devices generates vast amounts of data, previously only collected through direct contact with healthcare organizations. Nowadays, the role of the patient as an active partner in health care, rather than just a passive subject of diagnostic tests and medical treatments, is widely recognized. The emergence of various applications has enhanced healthcare engagement for individuals, promoting participation in personalized medicine systems. We highlight the most popular apps

⁹ ISO 10781:2023. Available at: <https://www.iso.org/ru/standard/84722.html> [Accessed 09th February 2024].

known for their functionality and capabilities in simplifying the doctor-patient relationship. Specialized apps popular amongst pregnant women to maintain pregnancy journals, store ultrasound scans, track doctor appointments, etc. Applications are actively developed and used for various purposes, including: 1) promoting a healthy lifestyle with physical activities, and nutrition monitoring; 2) managing chronic conditions like diabetes mellitus, bronchial asthma, and mental disorders; 3) medication reminders; 4) a rehabilitation comorbid with acceptance and commitment therapy (Kim, et al, 2021).

Moreover, various applications are being created for doctors to expedite searches for specialized literature and medication guidelines. Patients have access to apps integrating cloud storage for medical test results, digital assistants for healthy eating, disease-predicting chatbots, and services enabling remote communication between patients and healthcare providers or family doctors. Consequently, connected health technology is evolving, establishing an entire ecosystem (medical organization – doctor – patient) as a component of public health (Carroll, Kennedy & Richardson, 2016:67).

It is important to note that the accessibility of various devices raises concerns about their compatibility and the potential for systematizing data collected from diverse sources. Large-scale distribution of assorted gadgets has led to the emergence of a specific field known as mobile health (mHealth). Affordable wireless mobile devices and applications, increasingly accessible, have become widely used. Unlike traditional e-health that primarily focuses on static elements such as telemedicine and patient records, mHealth centers on dynamic aspects like symptom tracking, physical status monitoring, medication reminders, personalized support for chronic illnesses, and immediate access to health-related information (Stecher, et al, 2023).

Amid the COVID-19 pandemic, the delivery and access to health care have faced unique challenges, particularly during lockdowns. Physicians have had to provide healthcare services remotely and have embraced mHealth due to physical distancing restrictions. Additionally, mHealth apps utilize location data and proximity alerts to notify users if they have been in close contact with someone who later tested positive for COVID-19. These timely alerts empower individuals to self-isolate, seek testing, and inform their healthcare providers, contributing to breaking the chain of transmission. This technology also offers healthcare professionals the opportunity to remotely consult and share data with colleagues. Furthermore, mHealth not only enables patients to receive remote consultations but also enhances medication adherence and delivers disease education (Alsahli, Hor & Lam, 2023).

The “quiet” revolution that has evidenced digital transformation to be more than just a technological shift also influences both strategy and management tactics in the healthcare sector, necessitating adequate legal support (Angerer, Stahl, Krasniqi & Banning, 2022). It is vital to legally consolidate a digital doctor–patient communication since these relations involve key issues of medical liability and legal assessment of medical errors.

Moreover, the extensive involvement of nearly every aspect of private life including health status in the digital realm brings forth cyber-related threats and challenges. Integrating mHealth data into a single network enables personalized monitoring but also raises concerns about the security and privacy of such sensitive medical information. Various stakeholders such as insurance companies, banks, employers, etc., may seek access to this data. However, healthcare data breaches and cyber attacks have become increasingly prevalent. For example, Brno University Hospital in the Czech Republic fell victim to a recent ransomware attack through spear-phishing, resulting in the encryption of data across the entire hospital network. Other cyber attacks have targeted organizations such as the Hammersmith Medicines Research Group in the United Kingdom (a COVID-19 vaccine trial group), Paris Hospital Authority in France, Babylon Health (a hospital appointment and teleconsultation videoconferencing system) in the United Kingdom (Muthuppalaniappan & Stevenson, 2021).

In each of these cases, the operations of medical organizations were disrupted for some time, and additional resources were needed to restore records and electronic systems. Data breaches and security issues in healthcare have significant implications for confidentiality, integrity, and availability. The aftermath of cyber attacks on healthcare organizations includes a loss of trust, credibility, and confidence from stakeholders. Furthermore, these organizations may face financial impacts and regulatory sanctions if proper care and processes were not followed. Healthcare disruptions due to cyber attacks can also undermine a nation's overall healthcare policy, as the unavailability of healthcare systems could compromise citizens' right to health care.

While the introduction of various medical portable devices allows for remote information transmission (usually via Bluetooth) and leverages the Internet of Things (IoT), it also introduces cyber security risks, such as remote program hacking and device reconfiguration. The IoT involves similar elevated risks due to data transfer within a network of interconnected devices exchanging data. Specific mobile apps have been developed for use on small, wireless computing devices, such as smartphones. For example, medical/vital monitors designed for healthcare use on the body provide a precise real time tracking. The management systems and internal logistics within modern hospital institutions are increasingly built on the IoT-based technology (Haidhar Athir Mohd Puat & Nor Azlina Abd Rahman, 2020). However, this management model becomes susceptible to external influence, posing threats to both specific medical organizations and the entire healthcare system.

Legal aspects of digital health

Digital health is a broad concept that includes electronic health, mobile health, healthcare informatics, and other digital tools that contribute to the advancement of a wide range of healthcare services and public health. An analysis of international law has revealed several initiatives aimed at regulating digital health applications.

For instance, the General Digital Health Law, which regulates digital health applications, was presented in Mexico on December 15, 2023, marking the most ambitious draft initiative in the country. However, according to the International

Comparative Legal Guides expert analysis, it is unlikely that major regulations regarding digital health will be passed due to numerous controversial issues¹⁰.

In Germany, the Act on Secure Digital Communication and Applications in the Healthcare System (E-Health-Gesetz) of December 21, 2015¹¹ triggered a debate on digitization, data protection and health. Since then, the digitalization of the healthcare system has been promoted through various laws, including:

- The Appointment Service and Healthcare Supply Act (TSVG) of May 6, 2019¹²;
- The Act for More Safety in the Supply of Pharmaceuticals (GSAV) of August 9, 2019¹³;
- The Act to Improve Healthcare Provision through Digitalization and Innovation (Digital Healthcare Act – DVG) of December 9, 2019¹⁴;
- The Act for the Protection of Electronic Patient Data in the Telematics Infrastructure (Patient Data Protection Act – PDSG) of October 14, 2020¹⁵;
- The Act on Digital Modernization of Healthcare and Nursing (DVPMG) of June 3, 2021¹⁶.

The enacted laws have defined the system for electronic patient data, ensuring privacy protection guarantees; introduced legal incentives to hasten the adoption of medical electronic applications; established protective measures for IT structure development in German healthcare, introducing mandatory requirements for technological compatibility of various applications, databases, platforms, and services; included telemedicine in the list of services reimbursed by insurance organizations; implemented a mechanism to enhance digital literacy in healthcare and reinforce patient

¹⁰ International Comparative Legal Guides: Digital Health Laws and Regulations Report Mexico 2024. Available at: <https://iclg.com/practice-areas/digital-health-laws-and-regulations/mexico> [Accessed 06th February 2024].

¹¹ Deutscher Bundestag: Gesetz für Sichere Digitale Kommunikation und Anwendungen im Gesundheitswesen. Available at: <https://dip.bundestag.de/vorgang/gesetz-f%C3%BCr-sichere-digitale-kommunikation-und-anwendungen-im-gesundheitswesen-sowie/67134> [Accessed 03rd February 2024].

¹² Deutscher Bundestag: Gesetz für Schnellere Termine und Bessere Versorgung (Terminservice- und Versorgungsgesetz – TSVG). Available at: <https://dip.bundestag.de/vorgang/gesetz-f%C3%BCr-schnellere-termine-und-bessere-versorgung-terminservice-und-versorgungsgesetz/240321?term=TSVG&f.typ=Vorgang&rows=25&pos=1> [Accessed 03rd February 2024].

¹³ Deutscher Bundestag: Gesetz für Mehr Sicherheit in der Arzneimittelversorgung – GSAV. Available at: <https://dip.bundestag.de/vorgang/gesetz-f%C3%BCr-mehr-sicherheit-in-der-arzneimittelversorgung/243802> [Accessed 03rd February 2024].

¹⁴ Deutscher Bundestag: Gesetz für eine Bessere Versorgung durch Digitalisierung und Innovation (Digitale Versorgung-Gesetz – DVG). Available at: <https://dip.bundestag.de/vorgang/gesetz-f%C3%BCr-eine-bessere-versorgung-durch-digitalisierung-und-innovation-digitale-versorgung-gesetz/251761?term=DVG&f.typ=Vorgang&rows=25&pos=2> [Accessed 03rd February 2024].

¹⁵ Deutscher Bundestag: Gesetz zum Schutz Elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG). Available at: <https://dip.bundestag.de/vorgang/gesetz-zum-schutz-elektronischer-patientendaten-in-der-telematikinfrastruktur-patientendaten-schutz-gesetz/260962?term=PDSG&f.typ=Vorgang&rows=25&pos=4> [Accessed 03rd February 2024].

¹⁶ Deutscher Bundestag: Gesetz zur Digitalen Modernisierung von Versorgung und Pflege (Digitale Versorgung-und-Pflege-Modernisierungs-Gesetz – DVPMG). Available at: <https://dip.bundestag.de/vorgang/gesetz-zur-digitalen-modernisierung-von-versorgung-und-pflege-digitale-versorgung-und-pflege-modernisierungs-gesetz/272822?term=DVPMG&f.typ=Vorgang&rows=25&pos=3> [Accessed 03rd February 2024].

empowerment. The Russian legal policy could benefit from considering the German experience, given the national characteristics of public administration in the healthcare sector.

The opportunities presented by digitalization can guide strategic planning across various regulatory sectors. The Presidential Council for Strategic Development and National Projects endorsed the Passport for the priority project Digital Economy of the Russian Federation on June 04, 2019, Protocol No. 7. Despite the existence of various project subprograms, there is currently no dedicated strategic document for digital health in Russia, unlike in other countries.

Here is a summary of the main prospects of digital medicine and the challenges faced by modern legal regulation:

1. The use of big data in healthcare enables a significant shift in approaches to individual patient treatment. Data gathered from various electronic devices or entered into the digital sphere can be processed based on specified parameters. A defining characteristic of big data is that altering parameters leads to new outcomes, facilitating continuous work with big data to achieve desired results. Additionally, anonymizing big data ensures secure conditions for data subject.

The rise of large datasets has underscored the need for a comprehensive legal framework for big data. In 2018, the Russian Federation introduced Draft Law No. 571124-7 On Amendments to the Federal Law on Information, Information Technologies, and Information Protection¹⁷, which aimed to solidify the concept of “big user data” and determine the operator status for such data. However, the State Duma committee on Informational Policy, Technologies and Communications returned the draft for revision, and no further attempts were made to introduce the project to the country’s legislative body.

2. Big data serves as a foundation for artificial intelligence (AI), raising concerns about the involvement of healthcare professionals in the decision-making process. For instance, AI has been successfully employed in cancer risk prediction, risk factor identification, and differential diagnosis (Yang et al, 2022). It is important to distinguish between weak AI and strong AI. The former is viewed as a tool that assists doctors in problem-solving through technical devices, programs, and algorithms, enabling them to independently diagnose diseases and provide medical care without the need for fundamental changes in legislation. Strong AI involves the concept of a “digital doctor” – a mechanism capable of performing certain functions of a physician or replacing them entirely. However, the lack of uniform regulatory approaches has resulted in the lack of legislation in most countries worldwide. Nonetheless, a range of complex legal issues must be addressed in the nearest future, including intellectual property rights related to improved machine learning algorithm (where both programmers and doctors may be involved in the algorithm description), medical malpractice liability, and delineation of responsibilities between a physician and a digital doctor.

¹⁷ The State Duma of the Federal Assembly of the Russian Federation: Draft Law No. 571124-7. Available at: <https://sozd.duma.gov.ru/bill/571124-7> [Accessed 07th February 2024].

The integration of AI-powered clinical decision support systems and personal assistants in the treatment of various diseases, such as stroke, diabetes, and cancer, has revolutionized the processing of extensive patient data. For instance, a clinical decision support systems for monitoring cancer tumors rely on access to liquid biopsies and their digital representation. Within the healthcare sector, there is an imminent need to effectively manage global data to promote the cross-border exchange of significant healthcare information. Nonetheless, this initiative presents complex legal challenges. Notably, the Government of the Russian Federation has approved the Rules for Import and Export of Biological Materials Obtained in Clinical Trials of Medicinal Products for Medical Use into and from the Russian Federation¹⁸.

The increasing utilization of AI in healthcare has paved the way for advancements in related domains, such as:

– Translational bioinformatics encompasses the comprehensive analysis of statistical data, genomic information, and clinical records to bolster healthcare quality, accessibility, and efficiency. However, it is essential to address the absence of legislative frameworks concerning genomic techniques, particularly pertaining to human deoxyribonucleic acid (DNA) within the Russian Federation.

– Digital health information management plays a crucial role in strengthening internal processes within any healthcare organization. The concept of Digital Hospital has emerged to address numerous management challenges, including the medical personnel mobility.

– Virtual reality, augmented reality, and the metaverse have been increasingly integrated, with computer simulations being widely introduced (Bakshi et al, 2021:1326), gamification in healthcare management, and virtual sensory tests for patients with muscle fatigue¹⁹, among other applications. However, these technologies lack a specific legal framework within the Russian Federation.

3. Digital biomedicine involves various digital products and techniques, such as organ-on-a-chip technology (Driver & Mishra, 2023), virtual health assistants (Curtis, et al, 2021), bioprinting (Romanovskaya & Romanovskiy, 2023), brain-computer interfaces (BCI)²⁰, and digital biomedical devices like bionic prostheses²¹. However, the implementation of these advancements presents complex ethical challenges that necessitate a reassessment of fundamental human rights. For instance, the introduction

¹⁸ The Official Internet Portal for Legal Information: Decree of the Government of the Russian Federation No. 363 of March 14, 2022. Available at: <http://publication.pravo.gov.ru/Document/View/0001202203160001> [Accessed 06th February 2024].

¹⁹ Gottsegen, G. (2023) *How Virtual Reality and Augmented Reality in Healthcare Is Changing Medicine*. Available at: <https://builtin.com/healthcare-technology/ar-virtual-reality-healthcare> [Accessed 06th February 2024].

²⁰ Elon Musk's neurotechnology company, Neuralink, proposed to implant chips in human brains. According to Musk, the company has already had some success with monkeys in 2019-2021. In September 2023, the brain-chip startup has received approval from an independent review board to begin recruitment for the first human trial of its brain implant for paralysis patients. Available at: <https://neuralink.com/> [Accessed 06th February 2024].

²¹ Motorika, LLC is the Russian leader in the development and production of high-tech bionic prostheses. Available at: <https://motorica.org/home?ysclid=lpbled93662152565> [Accessed 06th February 2024].

of a brain-computer interface involves the insertion of small chips into the human brain to stimulate motor-related areas, unlike commonly used biomedical chips like microfluidic chips. The extensive use of such interfaces to enhance human intellectual capabilities and to blur the boundaries between the biological and digital realms gives rise to the concept of biodigital convergence (Peters, Jandrić & Hayes, 2021:377). This convergence describes the merging of biological and digital technologies, termed biodigital technologies, impacting both social and biological life by transforming it into a digital code. Bioprinting of organs, human tissues, and nerve cells is performed based on such digital code (Rad, et al, 2022). As these advancements progress, they are expected to encounter legal issues related to extending constitutional legal personality to models with intellectual abilities, addressing gene-based discrimination between individuals with innate and altered abilities, and defining boundaries for human rights such as the right to life, personal integrity, and privacy. Furthermore, companies have patented the creation of human digital virtual clones, replicating various social and psychological attributes of an individual²². AI technologies that promise more chatbots and replicas of deceased individuals transformed into a 3D shells have given rise to the concept of “digital immortality” (Hurtado, 2022).

The concept of digital human rights that involves a biomedical aspect is currently a topic of active discussion.

Conclusion

The large-scale digitalization of healthcare has the potential to revolutionize the entire public health system and elevate personalized healthcare to new heights. However, the full potential of individual biological, social, and mental aspects within the healthcare system is yet to be fully realized. Personal data, in its broadest sense, is becoming increasingly vital for both the economy, in light of the digital revolution, and for healthcare, where it is gaining prominence as a public policy priority. The heightened individualization aimed at enhancing digital patient interaction not only expands individual capabilities, but also emphasizes personal health responsibility. The emergence of new opportunities to establish control not only over treatment processes but also over entire lifestyles is targeted at preventing and reducing the impact of many diseases. This shift may lead to a reevaluation of health protection responsibilities, transferring some health status aspects from personal to the public sphere. However, this also raises concerns about social control over sensitive areas of private life.

The use of digital technologies to enhance healthcare provision stipulates various approaches to legal regulation. For instance, the adoption of new mobile applications will require amendments to Article 38 of the Federal Law No. 323-FZ of November 21, 2011 On Basics of Health Protection of the Citizens in the Russian Federation and the Nomenclature Classification of Medical Devices (approved by Order No. 4n of the

²² Ivanov, Y. (2017) System and Method for Using a Digital Virtual Clone as an Input in a Simulated Environment. US9959497B1 (Patent). Available at: <https://patents.google.com/patent/US9959497B1/en> [Accessed 06th February 2024].

Ministry of Health of Russia of June 6, 2012). Mere indication of the software used may not suffice for these documents; additional targeted changes, monitoring, and initiative from the Ministry of Health of Russia are required. Extensive work is also necessary to standardize technical requirements for the digitalization of the entire healthcare provision process, particularly in terms of a unified format for data input to ensure its usability for further processing. Given the global interest in processing healthcare big data, universalization should align with rules for cross-border data exchange. This comprehensive approach could help formulate more explicit recommendations for the organization of healthcare and the provision of healthcare services, considering different disease groups and patient classification.

A number of digital health aspects involve organizational improvement through the implementation of the federal project Digital Public Administration of the national program Digital Economy of the Russian Federation. This will require management decisions, and its legal formalization should be as part of an overall administrative reform, thus redefining the role of the Ministry of Health as an architect of public administration. While digitalization brings about decentralization, it does not entail the abandonment of the system of government agencies; rather, it drastically alters their management methods, shifting from an imperative approach to the principles of behavioral economics, focusing on personal interests through nudging rather than direct coercion.

Global trends such as brain chipping and introduction of EMR require careful ethical and legal consideration. Improving physician practice and enhancing patient convenience are primary objectives that involve addressing technical challenges to bring the entire information array to a “common denominator”. The Russian Federation has outlined the goal of creating USHIS as a global service to incorporate various resources and registers for multi-purpose data exchange. However, skeptics in countries with well-developed digital infrastructure doubt the feasibility of such unification. The integration of databases poses risks such as data breaches (theft), criminal cyber attacks, and violations by public authorities and healthcare professionals. The traditional provision of healthcare has long been based on trust through medical confidentiality, patient autonomy, and prioritizing patient interests. Disruptions to these fundamental principles may lead to patient uncertainty, information concealment, and a search for alternative healthcare, potentially leading to the emergence of fraudulent practices, facilitated by social networks. Addressing these challenges, such as ensuring patient familiarity with any access to their personal EMR and utilizing blockchain technologies for medical data storage, requires independent legal assessment.

A major challenge arises from the emergence of biodigital convergence, wherein total digitalization risks reducing a human personality to a model with its own serial number. Additive technologies to bioprint human tissues and organs are based on converting them into numerical codes and transmitting them over distances.

It is apparent that the aforementioned perspectives and similar ones call for an appropriate legal response, which is currently lacking in Russian legislation. The reforms

proposed by the Ministry of Health of Russia face challenges in terms of burden and time required to pass them through the legislative process. Some laws are notably outdated, particularly those related to the legal regulation of genomic technologies, while others necessitate major revisions and supplements, such as the Federal Law No. 152-FZ On Personal Data of July 27, 2006 concerning big data and EMR regulations on Electronic Medical Records (EMR). Comprehensive reforms would involve overhauling the entire healthcare legislation, with a novel Healthcare Code of the Russian Federation as the ultimate objective. Implementing these measures would require addressing major existential dilemmas with an active legal support and lawyer participation.

References / Список литературы

- Alsahli, S., Hor, S. & Lam, M. (2023) Factors Influencing the Acceptance and Adoption of Mobile Health Apps by Physicians During the COVID-19 Pandemic: Systematic Review. *JMIR Mhealth Uhealth*. (11), e50419. <https://doi.org/10.2196/50419>
- Angerer, A., Stahl, J., Krasniqi, E. & Banning, S. (2022) The Management Perspective in Digital Health Literature: Systematic Review. *JMIR Mhealth Uhealth*. 10(11), e37624. <https://doi.org/10.2196/37624>
- Bakshi, S.K., Lin, S.R., Ting, D.S.W., Chiang, M.F. & Chodosh, J. (2021) The era of artificial intelligence and virtual reality: transforming surgical education in ophthalmology. *British Journal of Ophthalmology*. 105(10), 1325–1328. <https://doi.org/10.1136/bjophthalmol-2020-316845>
- Birrer, A., He, D. & Just, N. (2023) The state is watching you – A cross-national comparison of data retention in Europe. *Telecommunications Policy*. 47(4), 102542. <https://doi.org/10.1016/j.telpol.2023.102542>
- Brahams, D. (1995) The medicolegal implications of teleconsulting in the UK. *Journal of telemedicine and telecare*. 1(4), 196–201. <https://doi.org/10.1177/1357633X9500100402>
- Burgess, Gluskin & Pinker, (2023) From bedside to portable and wearable: development of a conformable ultrasound patch for deep breast tissue imaging. *Molecular Oncology*. 17(10), 1947–1949. <https://doi.org/10.1002/1878-0261.13531>
- Carroll, N., Kennedy, C. & Richardson, I. (2016) Connected Community Healthcare Ecosystem (CCHE) for managing long-term conditions. *Gerontechnology*. 14(2), 64–77.
- Curtis, R.G., Bartel, B., Ferguson, T., Blake, H.T., Northcott, C., Virgara, R. & Maher, C.A. (2021) Improving User Experience of Virtual Health Assistants: Scoping Review. *Journal of Medical Internet Research*. 23(12), e31737. <https://doi.org/10.2196/31737>
- Drexler, M., Elsner, C., Gabelmann, V., Gori, T. & Münzel, T. (2020) Apple Watch detecting coronary ischaemia during chest pain episodes or an apple a day may keep myocardial infarction away. *European Heart Journal*. 41(23), 2224. <https://doi.org/10.1093/eurheartj/ehaa290>
- Driver, R. & Mishra, S. (2023) Organ-On-A-Chip Technology: An In-depth Review of Recent Advancements and Future of Whole Body-on-chip. *BioChip Journal*. (17), 1–23. <https://doi.org/10.1007/s13206-022-00087-8>
- Eysenbach, G. (2001) What is e-health? *Journal of Medical Internet Research*. 3(2), e20. <https://doi.org/10.2196/jmir.3.2.e20>
- Haidhar Athir Mohd Puat & Nor Azlina Abd Rahman (2020). IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy. *Journal of Physics: Conference Series*. (1712), 012009. <https://doi.org/10.1088/1742-6596/1712/1/012009>

- Hurtado, J.H. (2022) Envisioning postmortal futures: six archetypes on future societal approaches to seeking immortality. *Mortality*, 1–19. <https://doi.org/10.1080/13576275.2022.2100250>
- Kierkegaard, P. (2011) Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review*. 27(5), 503–515.
- Kim, O.T., Dadaeva, V.A., Telhigova, A.A. & Drapkina, O.M. (2021) Mobile medical applications: opportunities, problems and prospects. *Russian Journal of Preventive Medicine*. 24(7). 96–102. <https://doi.org/10.17116/profmed20212407196> (in Russian).
Ким О.Т., Дадаева В.А., Тельхигова А.А., Дранкина О.М. (2021) Мобильные медицинские приложения: возможности, проблемы и перспективы // Профилактическая медицина. Т. 24. № 7. 96–102. <https://doi.org/10.17116/profmed20212407196>
- Lin, M., Zhang, Z. & Gao, X., et al. (2023) A fully integrated wearable ultrasound system to monitor deep tissues in moving subjects. *Nature Biotechnology*. (42), 448–457. <https://doi.org/10.1038/s41587-023-01800-0>
- Margolis, R.E. (1994) Law and policy barriers hamper growth of telemedicine. *Healthspan*. 11 (10), 14–15.
- Mokhov, A.A. (2010) Electronic medical record as a factor in the development of healthcare and protection of the rights of Russian citizens. *Medical Law*. (1), 23–26. (in Russian).
Мохов А.А. (2010) Электронная медицинская карта как фактор развития здравоохранения и защиты прав российских граждан // Медицинское право. 2010. № 1. С. 23–26.
- Muthuppalaniappan, M. & Stevenson, K. (2021) Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *International Journal for Quality in Health Care. Journal of the International Society for Quality in Health Care*. 33(1), mzaa117. <https://doi.org/10.1093/intqhc/mzaa117>
- Peters, M.A., Jandrić, P. & Hayes, S. (2021) Biodigital Philosophy, Technological Convergence, and Postdigital Knowledge Ecologies. *Postdigital Science and Education*. 3(2), 370–388. <https://doi.org/10.1007/s42438-020-00211-7>
- Rad, M.A., Mahmodi, H., Filipe, E.C., Cox, T.R., Kabakova, I. & Tipper, J.L. (2022) Micromechanical characterisation of 3D bioprinted neural cell models using Brillouin microspectroscopy. *Bioprinting*. (25), e00179. <https://doi.org/10.1101/2021.08.17.456575>
- Romanovskaya, O.V. & Romanovsky, G.B. (2023) Legal regulation of additive technologies in modern biomedicine. *RUDN Journal of Law*. 27(1), 21–40. <https://doi.org/10.22363/2313-2337-2023-27-1-21-40> (in Russian).
Романовская О.В., Романовский Г.Б. Правовое регулирование аддитивных технологий в современной биомедицине // RUDN Journal of Law. 2023. Т. 27. № 1. С. 21–40. <https://doi.org/10.22363/2313-2337-2023-27-1-21-40>
- Sanders, J.H. & Bashshur, R.L. (1995) Challenges to the implementation of telemedicine. *Telemedicine Journal*. 1(2), 115–123.
- Staunton, C., Slokenberga, S. & Mascalzoni, D. (2019) The GDPR and the research exemption: Considerations on the necessary safeguards for research biobanks. *European Journal of Human Genetics*. 27(8). 1159–1167.
- Stecher, C., Pfisterer, B., Harden, S.M., Epstein, D., Hirschmann, J.M., Wunsch, K. & Buman, M.P. (2023) Assessing the Pragmatic Nature of Mobile Health Interventions Promoting Physical Activity: Systematic Review and Meta-analysis. *JMIR Mhealth Uhealth*. (11), e43162. <https://doi.org/10.2196/43162>
- Van Veen, E.-B. (2018) Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate. *European Journal of Cancer*. (104), 70–80. <https://doi.org/10.1016/j.ejca.2018.09.032>
- Wadmann, S., Hartlev, M. & Hoeyer, K. (2023) The life and death of confidentiality: A historical analysis of the flows of patient information. *BioSocieties*. (18), 282–307. <https://doi.org/10.1057/s41292-021-00269-x>

Williams, S. (2018) GDPR – not just an EU regulation? *The Lancet Oncology*. 19(10), e508. [https://doi.org/10.1016/S1470-2045\(18\)30696-X](https://doi.org/10.1016/S1470-2045(18)30696-X)

Yang, X., Mu, D., Peng, H., Li, H., Wang, Y., Wang, P., Wang, Y. & Han, S. (2022) Research and Application of Artificial Intelligence Based on Electronic Health Records of Patients with Cancer: Systematic Review. *JMIR Medical Informatics*. 10(4). e33799. <https://doi.org/10.2196/33799>

About the authors:

Olga V. Romanovskaya – Doctor of Law, Full Professor, Head of the Department of State and Legal Disciplines, Penza State University; 40 Krasnaya str., Penza, 440026, Russian Federation

ORCID: 0000-0002-4563-1725; ResearcherID: C-7120-2017; SPIN-code: 5496-7700

e-mail: pgu-gpd@yandex.ru

Georgy B. Romanovskiy – Doctor of Law, Full Professor, Head of the Department of Criminal Law, Penza State University; 40 Krasnaya str., Penza, 440026, Russian Federation

ORCID: 0000-0003-0546-2557; ResearcherID: S-7012-2016; SPIN-code: 2791-8376

e-mail: vlad93@sura.ru

Об авторах:

Романовская Ольга Валентиновна – доктор юридических наук, профессор, заведующая кафедрой государственно-правовых дисциплин, Пензенский государственный университет; 440026, Российская Федерация, г. Пенза, ул. Красная, д. 40

ORCID: 0000-0002-4563-1725; ResearcherID: C-7120-2017; SPIN-код: 5496-7700

e-mail: pgu-gpd@yandex.ru

Романовский Георгий Борисович – доктор юридических наук, профессор, заведующий кафедрой уголовного права, Пензенский государственный университет; 440026, Российская Федерация, г. Пенза, ул. Красная, д. 40

ORCID: 0000-0003-0546-2557; ResearcherID: S-7012-2016; SPIN-code: 2791-8376

e-mail: vlad93@sura.ru