Legal Issues in the Digital Age. 2024. Vol. 5. No 2.
Вопросы права в цифровую эпоху. 2024. Том 5. № 2.

IT, Industries, Law: Telemedicine

Research article
УДК: 340, 34.06
DOI:10.17323/2713-2749.2024.2.57.79

The Use of AI in Medicine: Health Data, Privacy Risks and More

Boris Aleksandrovich Edidin[1], Alexey Vasilievich Bunkov[2], Ksenia Vladimirovna Kochetkova[3]

[1, 2] ANO «IRI, Institute for Digital Content Support & Development», 6/1/2 Kadashevskaya Embankment, Yakimanka Area, Moscow 119017, Russia,

[3] MGIMO University, 76 Prospect Vernadskogo, Moscow 119454, Russia,

[1] b.edidin2018@gmail.com

[2] bunkov.a@iri.center

[3] kochetkova.k@iri.center, Author ID: 1033155, ORCID ID: 0000-0002-6254-9539, Scopus Author ID: 57223024821

Abstract

In the era of advancements in artificial intelligence (AI) and machine learning, the healthcare industry has become one of the major areas where such technologies are being actively adopted and utilized. The global health care sector generated more than 2.3 zettabytes of data worldwide in 2020. Analysts estimate that the global market for artificial intelligence (AI) in medicine will grow to $13 billion by 2025, with a significant increase in newly established companies. Artificial intelligence in medicine is used to predict, detect and diagnose various diseases and pathologies. The sources of data can be various results of medical research (EEG, X-ray images, laboratory tests, e.g. tissues, etc.). At the same time, there are understandable concerns that AI will undermine the patient-provider relationship, contribute to the deskilling of providers, undermine transparency, misdiagnose or inappropriately treat because of errors within AI decision-making that are hard to detect, exacerbate existing racial or societal biases, or introduce algorithmic bias that will be hard to detect. Traditional research methods, general and special ones, with an emphasis on the comparative legal method, were chosen. For the AI to work it needs to be trained, and it's learning from all sorts of information given to it. The

main part of the information on which AI is trained is health data, which is sensitive personal data. The fact that personal data is qualified as sensitive personal data indicates the significance of the information contained, the high risks in case it's leaking, and hence the need for stricter control and regulation. The article offers a detailed exploration of the legal implications of AI in medicine, highlighting existing challenges, the current state of regulation, and proposes future perspectives and recommendations for legislation adapted to the era of medical AI. Given the above, the study is divided into three parts: international framework, that will focus primarily on applicable WHO documents; risks and possible ways to minimize them, where the authors have tried to consider various issues related to the use of AI in medicine and find options to address them; and relevant case-study.

Keywords

health data; AI training; sensitive personal data; privacy; deanonymization; data quality; algorithms; World Health Organization.

For citation: Edidin B.A., Bunkov A.V., Kochetkova K.V. (2024) The Use of AI in Medicine: Health Data, Privacy Risks and More. *Legal Issues in the Digital Age,* vol. 5, no. 2, pp. 57–79. DOI:10.17323/2713-2749.2024.2.57.79

Introduction

AI-powered applications have demonstrated their potential to transform medical diagnosis, treatment plans, drug discovery and patient care. E.g., the use of ChatGPT-like solutions in health care has enormous potential to improve the patient-provider relationship, such as patient clinic letter writing, medical note-taking and consultation, etc. [Chen C.W., Walter P., Wei J.C., 2024].[1]

The top 5 countries in the use of AI in medicine currently are the USA (48%), UK (7%), Israel (6%), Canada (4%), China (3%) [Imameeva R.D., 2021: 34].

Russia is also one of the leading countries in digitalization in medicine, including the use of AI. In 2022 a unique digital library of anonym da-

[1] The use of ChatGPT is being actively discussed in other fields besides medicine, especially in education and law. For example, for three months, experts from ANO IRI tested ChatGPT for its possible use in analytical and legal applications. The neural network was studied "out of the box", i.e. without any additional customizations and technical integrations with other services. Available at: URL: https://ири.рф/news/eksperty-iri-protestirovali-ispolzovanie-chatgpt-v-sfere-yurisprudentsii-i-normotvorchestva/ (accessed: 12.03.2024)

tasets for the evaluation and training of neural networks started functioning in Moscow.[2] In July 2023, unique AI-based medical technologies were presented at the Russia-Africa Summit.[3] Moscow is already using 12 AI systems in healthcare, which are registered and approved by the Federal Service of Roszdravnadzor; most of them are neural networks that assist radiologists.[4] At the moment of writing, smart algorithms are already assisting doctors in finding pathologies in 21 clinical areas.[5]

As of May, 2024 a medical decision support system based on artificial intelligence has facilitated preliminary diagnoses in Moscow hospitals, amounting to 14 million diagnoses.[6] A digital assistant system called "TOP-3" which analyses the patient's health complaints and offers three preliminary diagnoses. The physician may then either concur with one of the proposed diagnoses or formulate an alternative. The service is capable of identifying 95% of the most common diseases. However, neural networks do not replace the role of the doctor; rather, they free up the time and attention of the specialist to examine the patient and communicate with them. Ultimately, the final decision is always at the discretion of the physician.

Yandex and Sechenov University have launched a cloud platform of medical data for scientists in Russia, with 18 million medical documents uploaded to it.[7] With its help, specialists will be able to quickly find relevant medical reports, test results, CT scans, X-rays and other information, the company assures. They specified the platform will help scientists to develop new drugs and treatment methods, and developers — to develop AI in the field of health care.

---

[2] Moscow opened access to a digital data library for developers of artificial intelligence services in medicine // Available at: URL: https://www.mos.ru/news/item/107729073/ (accessed: 12.12.2023)

[3] Available at: sberbank.ru/ru/sbertv/broadcast/article?video=XB3j0r&listId=2 (accessed: 12.12.2023)

[4] Available at: URL:

[5] https://www.rbc.ru/rbcfreenews/6463777c9a7947472428599e (accessed: 12.12.2023) 5 Ibid.

[6] Rakova claimed to make 14 million provisional diagnoses using AI // Available at: URL: https://www.rbc.ru/rbcfreenews/664cc2e99a7947847c959310 (accessed: 22.05.2024)

[7] Yandex and Sechenov University have created a medical data platform for scientists // Available at: URL: https://www.forbes.ru/tekhnologii/502840-andeks-i-secenovskij-universitet-sozdali-platformu-medicinskih-dannyh-dla-ucenyh?erid=LdtCKapuV (accessed: 22.12.2023)

One of the most recent advancements in the field of AI application in healthcare is an AI-based algorithm to create drugs. Russian researchers at ITMO University have developed AI-based algorithm that will simplify and reduce the cost of creating finished pharmaceutical forms.[8] The new solution will make it possible to generate auxiliary molecules with the desired properties and assemble the basis of a future drug before experiments are conducted.

AI can perform a large number of functions related to the automation of labor-intensive processes and assistance to the medical doctor, such as:

analyzing and processing data (to make possible diagnoses and conclusions, or to come up with personalized treatment (e.g. individual therapy plans, precise selection of drug dosages, etc.);

monitoring the effectiveness of the actions taken (assessment of treatment dynamics);

monitoring of the patient's condition, recording the indicators from body sensors or hospital equipment data;

interacting with patients and their relatives to collect primary information or counseling on standard issues;

exercising various auxiliary functions related to document management and medical staff activities, such as voice recognition systems for filling out medical records, medical histories and other documents.

As a separate direction, robotic surgery can be singled out, in which robots help out during operations both with the participation of a doctor (robots act as assistants) or entirely by themselves without human participation, for more common and "easy" surgical procedures.

Another area is conducting research in pharmacology and development of new drugs and vaccines [Thomas S., Abraham A. et al., 2022]; [McCaffrey P., 2022]; [Boniolo F., Dorigatti E. et al., 2021]. By implementing AI technologies, pharmaceutical companies are able to shorten drug development and clinical trials, thereby reducing the cost of launching new drugs, which also facilitates the production of high-quality drugs with fewer side effects [Alekseeva M.G., Zubov A.I., Novikov M. Yu., 2022: 11].

These are just a few examples of what artificial intelligence is being used for in healthcare (more uses see Fig. 1).

[8] An algorithm for fast drug formation with the help of AI created in St. Petersburg // Available at: URL: https://nauka.tass.ru/nauka/20046793?utm_source=yxnews&utm_medium=desktop&utm_referrer=https%3A%2F%2Fdzen.ru%2Fnews%2Fsearch%3Ftext%3D (accessed: 12.03.2024)

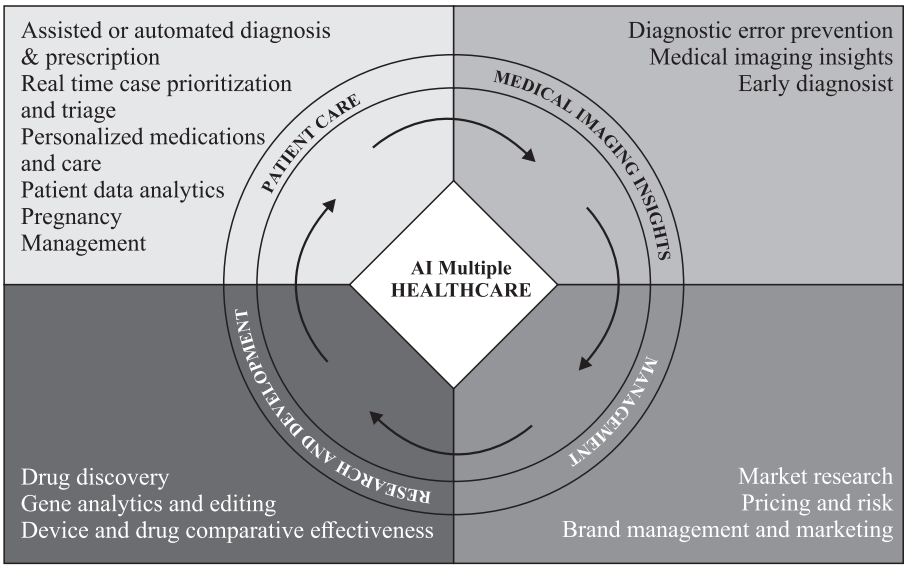

Fig. 1. AI Use Cases in Healthcare Industry in 2024[9]

All models, AI systems, algorithms depend on health data which comes from different sources:

clinical data (laboratory data, patient records and etc.);

genomic data (mostly means genetic testing);

imaging (results from X-ray, MRI, and other radiology diagnostics);

administrative data (not health data per se, but the information connected to a patient like financial statements, insurance, billing info, etc.);

sensors and wearables data.

Being a central element of the above-mentioned technologies is the use of huge amounts of medical data of patients, which is the basis for building any algorithm. And this vast amount of data shall be handled accordingly though its lifecycle (see Fig. 2).

However, the prospect of using AI in healthcare is accompanied by a number of legal[10] and ethical issues, in particular those related to the criticality for human health and life of any errors in decision-making, as well as the collection, storage and use of confidential patient information.

[9] Available at: Top 18 AI Use Cases in Healthcare Industry in 2024 (aimultiple.com), (accessed: 22.05.2024)

[10] The legal and policy issues around privacy and patient data affect both clinical AI and other health care AI systems [McNair D., Price W.N. 2019: 197].

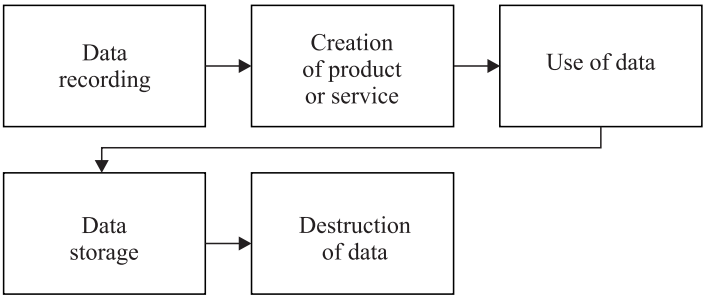

Fig. 2. Health Data Lifecycle

1. International Framework

As AI is a new and emerging technology, so far there is been no framework adopted on the issue. That is to say obligatory framework in the form of an international treaty that would regulate the use of AI. However, there are a number of soft-law documents on the issue.

At this point, the most extensive framework in a form of recommendation was provided by UNESCO as one of the specialized agencies of the UN. The paper "The Recommendation on the Ethics of Artificial Intelligence"[11] serves as an ethical guideline and helps to ensure strict adherence to the rule of law in the digital world. The document focuses on 11 Policy Areas, including "Health and Social Well-Being". As stated in Clause 122 (d): "Member States should pay particular attention in regulating prediction, detection and treatment solutions for health care in AI applications by ensuring effective mechanisms so that those whose personal data is being analyzed are aware of and provide informed consent for the use and analysis of their data, without preventing access to health care".[12]

Concerns about the introduction of AI in healthcare have been raised by another UN specialized agency — the World Health Organization (hereinafter WHO). First, in 2018 WHO has adopted a Resolution on Digital Health.[13] Among other things, the Resolution urges WHO Member States "to develop, as appropriate, legislation and/or data protection policies

[11] Recommendation on the Ethics of Artificial Intelligence // Available at: https://unesdoc.unesco.org/ark:/48223/pf0000381137_eng (accessed: 20.01.2024)

[12] Ibid.

[13] Seventy-first World Health Assembly, Agenda item 12.4 "Digital Health", 26 May 2018 // Available at: https://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf (accessed: 20.01.2024)

around issues such as data access, sharing, consent, security, privacy, interoperability and inclusivity consistent with international human rights obligations and to communicate these on a voluntary basis to WHO".

Later, following the Resolution of 2018, WHO Member States agreed on the Global Strategy on Digital Health for 2020–2025 which highlights the importance of AI.[14] As set forth in the Strategy, health data shall be classified as sensitive personal data and be attributed the highest possible safety and security standard (see page 11 of the document). Besides safety, Member States need to make sure the data is complete in its integrity. The Strategy points out that the use of health data to train AI is a secondary use of health data and shall be accompanied with appropriate deanonymization of datasets.

The WHO has also urged caution in using AI-generated large language model (LLM) tools to protect and promote human well-being, safety and autonomy, and to preserve public health. [15] It is noted that hasty implementation of unproven systems could lead to errors made by health professionals, or harm patients thus undermining trust in AI. Among the main concerns, WHO highlighted that the data used to train AI may be biased, creating misleading or inaccurate information.

Recently, in January 2024 the WHO has published framework "Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models".[16] The guide outlines more than 40 recommendations for consideration by governments, technology companies and healthcare providers to ensure the appropriate use of LMM to promote and protect public health. Among other things, the risks and potential benefits of LMM are described, and the following key recommendations are provided for LMM developers to ensure the following:

---

[14] Global strategy on digital health 2020-2025. Geneva: World Health Organization; 2021 // Available at: https://www.who.int/docs/default-source/documents/gs-4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf (accessed: 20.01.2024)

[15] WHO outlines considerations for regulation of artificial intelligence for health, October 2023 // Available at: https://www.who.int/news/item/19-10-2023-who-outlines-considerations-for-regulation-of-artificial-intelligence-for-health#:~:text=The%20World%20Health%20Organization%20(WHO),manufacturers%2C%20health%20workers%2C%20and%20patients (accessed: 20.01.2024)

[16] Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models // Available at: https://www.who.int/publications/i/item/9789240084759 (accessed: 05.02.2024)

LMMs are not only developed by scientists and engineers. Potential users and all direct and indirect stakeholders, including health care providers, academic researchers, healthcare professionals, and patients, should be involved early in the product development process.

LMMs must perform well-defined tasks with the necessary accuracy and reliability to improve the capacity of health systems and protect the interests of patients.

2. Risks and Possible Mitigating Measures

The following key risks associated with the use of AI in medicine can be identified:

a) Errors in AI algorithms

In addition to inaccurate and low-quality data on which AI is trained, errors can also occur in the algorithms themselves, for example, due to incorrect AI programming or failure to take into account any data used, which can lead to incorrect treatment recommendations or diagnoses. The issue here is the transparency of the algorithms and their ethical use.

b) Breach of privacy and data security

Accumulation and use of large amounts of patient medical data increase the risk of unauthorized access, breach of confidentiality and data leaks.[17] The legislation of the Russian Federation provides a number of mandatory requirements for information security in the collection and processing of personal medical data.

c) Risk of data deanonymization

Cleansing patient data from personal information does not guarantee anonymization, as artificial intelligence models can re-identify a person. In order to minimize this risk, an example of a possible practice may be the anonymization of personal data by mixing method (shuffle). In this case, the original field value of one record is replaced by a randomly selected value of the same attribute of another data record within the same dataset.

[17] For example, in the USA the HHS' Office for Civil Rights has reported over 239 breaches in 2023, affecting the health care data of more than 30 million individuals within the U.S. See: B. Lewis. Navigating Health Data Privacy in AI-Balancing Ethics and Innovation. Available at: https://www.lexology.com/library/detail.aspx?g=19c61aa9-3e34-4894-84b4-81d814de926c (accessed: 20.01.2024)

The serious limitation of this method is the unsuitability of "shuffled" data for the search of possible correlations.

d) Data quality, validity and relevance.

A substantial barrier to innovation in healthcare seems to be the availability of high-quality data on which to train AI, which limits the types of users who can successfully innovate [Price W.N., Sachs R., Eisenberg R.S., 2021:39]. To ensure data quality, reliability and relevance, a number of principles and sequences must be followed. In the course of the performance the following should be provided:

definition of the goals and objectives of data collection, the planned ways of their subsequent use and the tools used in this process, the planned volume of data to be collected;

preparing a statement of work or other structured description of the data collection requirements, which includes the requirements for the planned result;

collecting raw data from various sources and determining the sources of information, their reliability, and the type of data to be collected. Algorithm developers need to assemble data from multiple sources to train machine learning algorithms. Those data — as well as data about how the algorithms perform in practice – may then be shared with other entities in the healthcare system for the purpose of evaluation and validation [Price W.N., 2017: 13]. For example, the "Regulations for the preparation of datasets describing approaches to generating a representative sample of data" distinguish the following types of data used in medical AI: medical records, electronic medical records, laboratory data, medical images, genomics, auxiliary data;[18]

data annotation and data markup. Annotation and markup refer to the processing of raw data for the purposes of its use in machine learning, in which the data is assigned a label or tag that allows algorithms to classify the received and processed information. The outcome of partitioning is the presence of fixed patterns in the data and its characteristics. This allows machine learning models to further interpret and sort incoming data. This is one of the key and labor-intensive stages of AI training work. According

[18] Prepared by the State Research and Practical Clinical Center for Diagnostics and Telemedicine Technologies, Moscow Health Department. Available at: URL: https://telemedai.ru/biblioteka-dokumentov/reglament-podgotovki-naborov-dannyh-s-opisaniem-podhodov-k-formirovaniyu-reprezentativnoj-vyborki-dannyh-chast-1-1 (accessed: 20.01.2024)

to the research by Cognilytica, preparing a dataset can take up to 80% of the total development time of an AI solution: e.g. in video annotation each hour of video requires about 800 man-hours.[19]

The organization of the data annotation and markup process should take into account:

availability of a sufficient number of qualified personnel, taking into account the planned volumes of annotation;

refusal to use outsourcing and crowdsourcing for medical data processing due to increased risks of leaks and possible low quality of the final result;

use of Russian software for data annotation and markup;

prohibition of remote work with data (e.g., when employees work on their personal devices from home). Thus, working in a secure corporate network is essential;

training of employees responsible for data annotation and markup;

feedback between the team of employees responsible for data annotation and markup and the teams that train and use the trained models to clarify and update the procedures for working with data, to quickly take into account necessary changes, to take into account the identified errors and the possibility of their prompt correction.

correct data entry into the system (correct and accurate description, no duplication of data, etc.). This shall be accompanied by reducing the impact of human factor: it's highly recommended to use automated data entry and verification, or independent verification by other specialists);

regular data auditing/verification/updating. In addition to internal verification, an external audit by an independent third party is recommended. One option would be to establish a system of licensed organizations authorized to conduct this type of audit;

data cleansing. Data cleansing involves identifying and correcting any errors or inconsistencies in the data. Data cleansing shall be performed by automated tools. However, in order to ensure data cleansing quality, it is advisable to provide for random checks by specialists. Cleansing should result in: deletion of duplicate data; deletion of data not related to the dataset; identification of missing data (ensuring data completeness); standardization of data — unified standards of data recording, transformation of data

[19] Cognilytica White Paper AI Data Engineering Lifecycle Checklist Following Steps for AI Project Success, 2020 // Available at: https://www.cloudera.com/content/dam/www/marketing/resources/whitepapers/ai-data-lifecycle-checklist-cloudera-whitepaper.pdf?daqp=true%20. (accessed: 20.01.2024)

into selected standards. This point is most critical if the data set is collected from different sources. Data cleansing can be broken down into the following steps: parsing; correcting; standardizing; matching; consolidating [Stöger K., Schneeberger D., Kiesebergc P., Holzinger A., 2021].

Competence Substitution (leading to medical negligence).

The frequent use of AI systems by a specialist creates a technology dependence, which can potentially lead to a loss of skills and abilities among medical staff, and a shift of responsibility for decision-making in the medical system. This can be particularly critical in the event of system failure or malfunction and the need for rapid decision making.

These risks can be minimized both at the regulatory level and at the level of the medical facility itself.

In the first case, it is necessary to legally establish the use of AI in healthcare (for example, by adding Article 36.3 "Peculiarities of Medical Care Provided Using Artificial Intelligence" to the Federal Law "On Basics of Health Protection of Citizens in the Russian Federation"), as well as to establish the criminal liability of a doctor for the final decision made using AI tools.[20] It has been supported by some specialists, who point out that medical doctors and hospitals that use AI bear the ultimate responsibility for its use, however, they need to be trained accordingly [Naik N. et al., 2022].

The second case requires regular training of personnel on how to work with the results obtained, as well as verification of decisions made by the doctor (e.g., random verification of decisions by an independent medical commission on a regular basis).

At the moment there is no unified approach to the issue of liability for errors resulting from the use of AI in medicine. A diagnosis founded upon AI technology offers an array of issues that are difficult to remedy through present concepts of responsibility [Hodge S.D., 2022: 436]. Some researchers assume that certain AI models should be given a unique legal status akin to personhood to reflect its current and potential role in the medical decision-making process, thus clearing who should bear responsibility and for what [Chung J., Zink A., 2018: 1]. The national legislation of some states is trying to find a solution, but it is still at the draft stage. An interesting approach in this context is that of Brazil, where a bill on AI use by doctors,

[20] Federal Law of 21.11.2011 No. 323-FZ // Available at: URL: https://www.consultant.ru/document/cons_doc_LAW_121895/ (accessed: 02.03.2024)

lawyers, and judges is under consideration by the National Congress.[21] The bill allows the use AI systems by doctors if it is under the doctor's supervision and the doctor's autonomy is preserved. The use of AI without such supervision would be considered as illegal medical practice.

The recently adopted European Union AI Act[22] also refers to the use of AI in healthcare. However, it does not directly cover the issues of responsibility for AI decisions and diagnoses by doctors, the Act still has some implications for the health sector. That being said, the Act classifies as high-risk AI systems those that could have a significant impact on human health and safety. AI Act mandates strict compliance for high-risk systems in terms of testing, documentation and transparency. The EU AI Act is founded upon a commitment to the upholding of ethical principles and the protection of fundamental human rights. The Act mandates that AI systems, especially those used in healthcare, are developed and deployed in a manner that respects human dignity, autonomy and privacy.

A similar approach has been effectively adopted by European Union GDPR: its Article 22 regulates decisions based solely on automated processing.[23] As it has been argued, this could be interpreted as to establish a "right to information and explanation, and therefore entail that "black box" systems, which do not allow any "meaningful human control", nor any explanation, should be prohibited.[24]

The use of AI in medicine, in addition to the above, also raises the following questions: Who is responsible for algorithm development? Is phased implementation with testing necessary? Are there market authorization procedures and is there certification? Are there regulations for identifying

---

[21] Projeto de lei No. 266, de 2024 sobre o uso de sistemas de inteligência artificial para auxiliar a atuação de médicos, advogados e juízes // Available at: https://legis.senado.leg.br/sdleg-getter/documento?dm=9547216&ts=1708613219368&disposition=inline (accessed: 02.03.2024)

[22] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts // Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (accessed: 21.05.2024)

[23] The General Data Protection Regulation (Regulation (EU) 2016/679) // Available at: https://gdpr.eu/article-22-automated-individual-decision-making/ (accessed: 10.04.2024)

[24] Verdicchio M., Perin, A. When Doctors and AI Interact: on Human Responsibility for Artificial Risks // Available at: https://link.springer.com/article/10.1007/s13347-022-00506-6#citeas (accessed: 10.04.2024)

and responding to errors and incidents? Who is responsible for identifying errors?

We now propose to consider each issue separately.

a) Who is responsible for algorithm development?

The price of error in the operation of such algorithms is extremely high. Algorithms can be developed and written by both companies and developers. Proper certification of companies and accreditation of developers would be an essential prerequisite. A "Personal license" system may be established to ensure the traceability of specialists' involvement in algorithms development.

b) Is a phased implementation with testing necessary? Are there market authorization procedures?

These two issues are closely interlinked and should be addressed together. Medical devices using AI are subject to mandatory testing and registration. Authorization procedures are available and are generally related to the production of medical devices (hereinafter — MD) and the requirements for their production.

By the Federal Law No. 323 medical devices also include "special software". The criteria for classifying software as a medical device are set out in one the Roszdravnadzor's information letters.[25] Such criteria include the following points:

the software is a computer program or its module regardless of the hardware platform, methods of placing the software and providing access to it;

the software is not an integral part of another MD;

the software is intended by the manufacturer to provide medical care;

the result of the software is interpretated in an automatic mode, including the use of artificial intelligence, and this result influences clinical decision-making.

In the case of qualifying, according to the criteria, MD as software, it is necessary to determine the class of risk to which such MD belongs (see Order of the Ministry of Health No. 4 of 06.06.2012[26]). In accordance with

[25] On Software. Roszdravnadzor letter of 03.02.2020 No. 02I-297/20 // Available at: URL: https://www.garant.ru/products/ipo/prime/doc/73467702/ (accessed: 02.03.2024)

[26] Order of the Ministry of Health No. 4n 06.06.2012 "On Approval of Nomenclature Classification of Medical Devices" (together with Classification of Medical

Section III of Annex 2 to this Order, the following classes of potential risk are distinguished:

Class 1 — low-risk software;

Class 2a — software with medium risk degree;

Class 2b — high-risk software;

Class 3 — the highest-risk software.

According to clause 15.1.1., software with the use of AI technologies belongs to class 3.

After determining the risk class, the developer (manufacturer) must conduct technical and clinical trials regulated by the Russian Ministry of Health.[27] It is worth bearing in mind that these tests are conducted not by the developer, but by third parties that are independently determined by the developer: separately by a testing organization and separately for clinical trials by a medical body. Requirements for medical bodies conducting clinical trials are approved by Order of the Ministry of Health.[28] A list of medical organizations meeting these requirements is available on the website of Roszdravnadzor.[29]

After the tests have been carried out and a full set of documents has been drawn up, the developer must register its AI-based medical device. According to Clause 4 of Article 38 of the Federal Law No. 323, the circulation of registered medical devices is allowed on the Russian territory. Clause 15 of Article 38 establishes a ban on the production of: 1) medical devices not included in the state register of medical devices and organizations (individual entrepreneurs) engaged in the production and manufacture of medical

---

Devices by Type, Classification of Medical Devices by Class depending on the potential risk of their use") // Available at: URL: https://www.consultant.ru/document/cons_doc_LAW_132477/ (accessed: 02.03.2024)

[27] Order of the Ministry of Health No. 885n of 30.08.2021 "On Approval of the Procedure for Conformity Assessment of Medical Devices in the Form of Technical Tests, Toxicological Studies, Clinical Tests for the Purpose of State Registration of Medical Devices" // Available at: URL: https://www.garant.ru/products/ipo/prime/doc/402937444/ (accessed: 02.03.2024)

[28] Order of the Ministry of Health of the Russian Federation No. 300n of 16.05.2013 "On Approval of Requirements for Medical Organizations Conducting Clinical Trials of Medical Devices and the Procedure for Establishing Compliance of Medical Organizations with These Requirements" // Available at: https://base.garant.ru/70585522 (accessed: 02.03.2024)

[29] List of medical organizations conducting clinical trials of medical devices // Available at: https://roszdravnadzor.gov.ru/services/clinicaltrials (accessed: 02.03.2024)

devices, except for medical devices produced for testing and (or) research; 2) falsified medical devices. Thus, it is prohibited to manufacture medical devices that have not been entered in the state register. Registration of medical devices is carried out by Roszdravnadzor, according to the Resolution of the Government of the Russian Federation No. 1416 of December 27, 2012 "On Approval of the Rules of State Registration of Medical Devices", and information about registered MIs is placed in a special register.[30]

c) Are there regulations for identifying and responding to errors and incidents?

Obviously, it is necessary to develop requirements at the federal level for organizational and technical measures to detect and respond to errors and incidents in organizations using IT solutions based on artificial intelligence. The established requirements should be implemented at the level of each organization that develops and maintains or uses IT solutions based on artificial intelligence.

d) Who is responsible for identified errors?

One of the key principles of decision making, especially in controversial situations, should be the principle of the responsibility of the specific person making that decision. Before registration and production, at the stage of technical and clinical trials, no real decisions should be made. After the registration of a software product or hardware-software complex and its release on the market, there should be mandatory responsibility of an authorized employee at every stage of the system that uses artificial intelligence in its work.

3. National Models

In 2021, AI in healthcare market was worth around 11 billion U.S. dollars worldwide.[31] The Global AI in Healthcare Market was estimated to be 14.41 billion U.S. dollars in 2023 and is expected to reach 51.07 billion U.S. dollars by 2028.[32]

[30] State register of medical devices and organizations (individual entrepreneurs) engaged in the production and manufacture of medical devices // Available at: URL: https://roszdravnadzor.gov.ru/services/misearch (accessed: 02.03.2024)

[31] Artificial intelligence (AI) in healthcare market size worldwide from 2021 to 2030 // Available at: URL: https://www.statista.com/statistics/1334826/ai-in-healthcare-market-size-worldwide/ (accessed: 10.04.2024)

[32] Global AI in Healthcare Market (2023-2028) by Sections, Diagnosis, End user and Geography. IGR Competitive Analysis, Impact of Covid-19, Ansoff Analysis //

Below authors of article offer a closer look at implementation practices in the United States and China, including real-life cases and projects by big tech companies. Jurisdictions were selected based on the worth of AI market in health care and most elaborative framework.

3.1. US Model

It was forecast that the global healthcare AI market would be worth almost 188 billion U.S. dollars by 2030, increasing at a compound annual growth rate of 37 percent from 2022 to 2030.[33]

The US is the leader in terms of AI investment and number of medical databases in the world. US AI in the healthcare market is projected to grow to 51.3 billion U.S. dollars by 2030.[34]

Surely, the number of digitized health data has recently grown, attracting new companies to the health data ecosystem. Technology start-ups, in addition to IT giants such as Google, Apple, and IBM, collect data through the use of apps, their online search platforms, and an ever-expanding array of health technology devices (e.g., sleep trackers, electrocardiograms, smart thermometers, etc.)[35]

For instance, in 2015, Google's DeepMind Health AI entered in partnership with a National Health Services hospital system in the UK and shared 5 years of identifiable medical data on 1.6 million patients. Later, the UK regulator (ICO) concluded that the companies failed to comply with data protection laws, especially considering the sensitive subject matter — health data.

Nuance is an AI-powered voice recognition company that serves healthcare alongside other verticals like security and customer engagement. It works for both telehealth and inperson consultations, and it raised 69.4 million U.S. dollars of investment before being acquired by Microsoft.

Available at: https://www.researchandmarkets.com/reports/5451294/global-ai-in-healthcare-market-2023-2028-by (accessed: 10.04.2024)

[33] Ibid.

[34] US Artificial Intelligence (AI) in Healthcare Market Analysis // Available at: https://www.insights10.com/report/us-artificial-intelligence-ai-in-healthcare-market-analysis/#:~:text=US%20Artificial%20Intelligence%20(AI)%20in%20the%20healthcare%20market%20is%20projected,forecast%20period%20of%202022-30. (accessed: 10.04.2024)

[35] Winter J.S. 2021. AI in healthcare: data governance challenges // Available at: https://jhmhp.amegroups.org/article/view/6448/html (accessed: 10.04.2024)

In the absence in the US a federal law on personal data protection, the main regulation for medical data is encompassed in the Health Insurance Portability and Accountability Act (otherwise known as HIPPA).[36] HIPPA's provisions establish standards for protection of personal health data, or as used in the Act — "protected health information, PHI", collected by covered entities. Covered entities, in turn, include hospitals, clinicians, or insurers, which means that HIPAA protects only this limited area of health information. [Spector-Bagdady K., Armoundas A.A., et al. 2023:1063]

PHI refers to any information in a medical record or data set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a healthcare service, such as diagnosis or treatment. HIPAA and regulations related thereto permit researchers to access and use PHI when necessary. Use of AI in healthcare is not directly mentioned in HIPPA, however as AI becomes increasingly prevalent in healthcare, it is vital to prioritize compliance with the HIPAA. Since HIPAA also establishes the standard for safeguarding medical information in the United States, ensuring the confidentiality, integrity, and availability of all electronic protected health information (ePHI). Given the nature of AI applications, which often involve handling sensitive health data, it is crucial for these applications to adhere to these regulations.

The states have been repeatedly trying to come up with federal privacy law. Today there are separate laws on state level regulating the following: consumer privacy, medical data, genetic data (separate from "general" medical, since it is more sensitive and requires additional oversight), consumer protection. The most recent try is under consideration by the US Congress. The new privacy bill[37] is not unlike previous similar bills and incorporates concepts that are familiar to companies and users from state data protection laws. Most importantly, if enacted, it would repeal and replace all US states data protection laws that have come into force in recent years, such as those of California, Colorado, Virginia, and others.

According to the Bill, personal data ("covered data" in the Bill's wording) includes any information that identifies or is associated, together or in combination with other information, with a natural person or a device that

[36] Available at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (accessed: 10.04.2024)

[37] A Bill to Establish Protections for Covered Data of Individuals, and for Other Purposes // Available at: https://www.commerce.senate.gov/services/files/3F5EEA76-5B18-4B40-ABD9-F2F681AA965F (accessed: 10.04.2024)

identifies or is associated with one or more persons. The Bill also creates a "subcategory" of personal data deemed sensitive, that is subject to additional and heightened requirements. The definition of "sensitive data" is much broader than in other data protection laws and includes: physical or mental health information; genetic information; biometric information.

To summarize, companies that are subject to HIPAA and comply with its rules would be deemed to be in compliance with similar provisions of the proposed Bill. However, if a healthcare company is subject to the Bill, it would also be required to comply with the Bill's data privacy provisions.

In addition to the above, the US government is actively investing in the private sector. The 2023 Executive Order set a goal to "accelerate grants" awarded to develop AI systems in healthcare.[38] Furthermore, the Order outlines the necessity to improve "healthcare-data quality to support the responsible development of AI tools for clinical care".[39]

3.2. China Model

According to the recent research, Chinese AI in healthcare market was valued at 0.07 billion U.S. dollars and is expected to grow significantly at a compound annual growth rate (CAGR) of 52.8% from 2020 to 2028.[40] Other statistics shows that the Chinese market was projected to reach 11.91 billion U.S. dollars by 2030.[41] As of 2021, an investment of approximately 60 billion yuan (9 billion U.S. dollars) had only been made in the field of smart medicine in China.

Some of the major players include Google Health, Tencent Trusted Doctors and NERVTEX. Among the world's top 20 cities in terms of AI companies hosted, Beijing ranks first with 395 companies, and Shanghai,

[38] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 2023 // Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (accessed: 10.04.2024)

[39] Ibid.

[40] China AI in Healthcare Market Size and Trends to 2031 // Available at: https://www.linkedin.com/pulse/china-ai-healthcare-market-size-trends-2031-cv2ye (accessed: 10.04.2024)

[41] China Artificial Intelligence (AI) in Healthcare Market Analysis // Available at: https://www.insights10.com/report/china-artificial-intelligence-ai-in-healthcare-market-analysis/ (accessed: 10.04.2024)

Shenzhen and Hangzhou are also among the top 20.[42] AI is being deployed across the healthcare industry in areas such as medical imaging devices, diagnostics and drug discovery.[43] .

Over the last 10 years China adopted a range of regulations and guidelines on the topic. It first started with 2016 document of the use of big data for the healthcare industry[44]. The Opinion outlined the following:

the integration of nationwide and provincial healthcare platforms with the online drug tender platform in 2017;

the establishment of a classified open platform for nationwide health information in 2020;

the sharing of basic data on the population, legal persons and geographic location between ministries and regions;

the establishment of 100 clinical data sample centres;

the creation of an electronic health archive for citizens; and

the introduction of a healthcare card.[45]

Then in 2017 the Ministry of Industry and Information Technology issued a three-year AI action and implementation plan[46], fostering the development of smart products in healthcare.

In 2021 State Food and Drug Administration has issued a Guidance for classifying and defining medical software products with artificial intelligence.[47] The document sets out the classification, registration, filing and clinical evaluation requirements for AI medical software products. Moreover, the Guidance defines "medical device data" as information generated

[42] China AI in Healthcare Market Size and Trends to 2031 // Available at: https://www.linkedin.com/pulse/china-ai-healthcare-market-size-trends-2031-cv2ye (accessed: 10.04.2024)

[43] How AI is shaping these three industries in China // Available at: https://www.jpmorgan.com/insights/global-research/artificial-intelligence/ai-transforming-industries-in-China (accessed: 20.05.2024)

[44] Opinion on the Promotion and Standardisation of Application and Development of Big Data for the Healthcare Industry, 2016 // Available at: https://www.gov.cn/zhengce/content/2016-06/24/content_5085091.htm (accessed: 10.04.2024)

[45] China Releases New Opinion to Promote Big Data in Healthcare // Available at: https://cms.law/en/chn/publication/china-releases-new-opinion-to-promote-big-data-in-healthcare (accessed: 10.04.2024)

[46] Available at: https://www.cac.gov.cn/2017-12/15/c_1122114520.htm (accessed: 10.04.2024)

[47] Available at: https://www.nmpa.gov.cn/ylqx/ylqxggtg/20210708111147171.html?type=pc&m= (accessed: 10.04.2024)

by medical devices, thus directly creating two categories of data — already gathered medical data and so-called secondary data that is produced by the devices itself (obviously, based on initial data).

There are 3 categories of key stakeholders in development of AI healthcare:

a) Governmental stakeholders:

The Shanghai Hospital Development Centre (SHDC) is currently implementing a Hospital Link Project with the primary objective of establishing a network of interconnected systems that will facilitate the real-time sharing of data and information between all hospitals in Shanghai.

The Chinese Innovative Alliance of Industry, Education, Research and Application of Artificial Intelligence for Medical Imaging has published a number of consensus documents on topics related to AI. One such document is the 2019 White Paper on Medical Imaging Artificial Intelligence in China, which serves as a reference point for understanding market demands and establishing standardised systems in the field of medical imaging, with the objective of facilitating the introduction of AI products.

b) Academic stakeholders

Academic stakeholders — mostly research institutes in the field of engineering, life science and physical science needed to research to solve problems in biomedicine: Med-X, Shenzhen Institutes of Advanced Technology of the Chinese Academy of Sciences, and Shanghai Institute of Materia Medica.

c) Tech companies

Chinese technology companies, such as Tencent and Alibaba, have begun to recognize the challenges facing the healthcare sector as an opportunity to leverage their consumer-oriented approach, which is focused on meeting the diverse demands of consumers across multiple contexts and channels, in order to capture a new market for digital healthcare solutions. Although physicians, hospitals, and other healthcare providers possess greater experience working within a heavily regulated environment and are able to deliver high-acuity care, these technology companies have the advantage of being able to innovate, scale up, and respond rapidly to market demands, as well as benefiting from a deep understanding of consumers. This has positioned them well to meet the basic healthcare needs of a significant proportion of the population.

Tecent is pursuing a strategy to transform hospitals into Smart Hospitals. This strategy enables patients to schedule appointments with specialists, conduct virtual visits, and access personal health information such as diagnostics, imaging reports, and prescriptions.

Alibaba employs its logistics expertise to facilitate the expedient delivery of pharmaceuticals procured from partner pharmacies within a timeframe of less than 24 hours. In order to gain a greater share of the value chain, Alibaba established its Tmall pharmacy division with the objective of distributing over-the-counter drugs and medical devices to consumers.

A prediction model was constructed by Ping An Technology using case reports from participating hospitals, historical data from regional health authorities and meteorological and environmental statistics. This model was designed to predict flu outbreaks with an accuracy rate of over 90%. The company also created "one-minute clinics" — small rooms or booths where patients enter to connect with an AI doctor that in a few minutes offers a preliminary diagnosis of ailments.[48]

Conclusion

The use of AI in healthcare is coupled not only with benefits, but also with a number of pitfalls. In order to erase these pitfalls, mitigate the identified risks and increase the potential benefits, we are in crucial need for legal regulation.

The above-mentioned measures for risk mitigation can be included in strategic documents on the use of artificial intelligence in healthcare, taken into account in local acts of medical and research institutions, as well as developers of systems using artificial intelligence.

Preparing large verified academic datasets is a lot of work and it is expensive to say the least. For this purpose, BRICS and its health committee (BCICH) or the BRICS Academic Forums could serve as a discussion platform for these issues with further elaboration of international regulation, especially considering recent expansion of BRICS members.

[48] Integrated Healthcare: A New Insurance Model in China // Available at: https://group.pingan.com/media/perspectives/Integrated-Healthcare-A-New-Insurance-Model-in-China.html (accessed: 10.04.2024)

References

1. Alekseeva M.G., Zubov A.I., Novikov M. Yu. (2022) Artificial Intelligence in Medicine. *Mezhdunarodnyi nauchno-issledovatel'skii zhurnal*=International Research Journal, no. 7, pp. 10–13 (in Russ.)

2. Boniolo F. et al. (2021) Artificial Intelligence in Early Drug Discovery Enabling Precision Medicine. *Expert Opinion on Drug Discovery*, vol. 16, no. 9, pp. 991–1007. DOI: https://doi.org/10.1080/17460441.2021.1918096

3. Chen C.W., Walter P., Wei J.C. (2024) Using ChatGPT-Like Solutions to Bridge the Communication Gap Between Patients With Rheumatoid Arthritis and Health Care Professionals. *Journal of Medical International Research Medical Education*. Available at: https://doi.org/10.1186/s13643-022-01939-y (accessed: 16.05.2024)

4. Chung J., Zink A. (2018) *Asia Pacific Journal of Health Law & Ethics*, vol.11, no. 2, pp. 51–80.

5. Da Silva M. et al. (2022) Legal Concerns in Health-Related Artificial Intelligence: a Scoping Review Protocol. *Systematic Reviews,* no. 11. Available at: https://doi.org/10.1186/s13643-022-01939-y (accessed: 18.07.2023)

6. Hodge S.D. (2022) The Medical and Legal Implications of Artificial Intelligence in Health Care — An Area of Unsettled Law. *Richmond Journal of Law & Technology,* vol. XXVIII, issue 3, pp. 405–468.

7. Imameeva R.D. (2021) The Risks of Creation and Functioning of Artificial Intelligence in Medicine. *Vestnik Moskovskogo universiteta imeni S. Yu. Vitte. Seriya 2: Yuridicheskie nauki*=Bulletin of Moscow Witte University. Series 2: Legal Science, no. 1, pp. 33–40. DOI: 10.21777/2587-9472-2021-1-33-40 (in Russ.)

8. McCaffrey P. (2022) Artificial Intelligence for Vaccine Design. *Methods in Molecular Biology*, vol. 2412, pp. 3–13. DOI: 10.1007/978-1-0716-1892-9_1

9. McNair D., Price W.N. (2019) Health Care AI: Law, Regulation, and Policy. In: Artificial Intelligence in Health Care: The Hope, the Hype, the Promise, the Peril. M. Matheny et al. (eds.) Washington: National Association of Medicine, pp. 181–213.

10. Naik N. et al. (2022) Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility? *Frontiers in Surgery,* vol. 9. DOI: https://doi.org/10.3389/fsurg.2022.862322

11. Price W.N. (2017) Artificial Intelligence in Health Care: Applications and Legal Implications. *The SciTech Lawyer,* vol. 14, no. 1.

12. Price W.N., Sachs R., Eisenberg R.S. (2021) New Innovation Models in Medical AI. Law & Economics Working Papers. 47 p.

13. Spector-Bagdady K., Armoundas A.A. et al. (2023) Principles for Health Information Collection, Sharing, and Use: A Policy Statement From the American Heart Association. Circulation, vol. 148, pp. 1061–1069. DOI: 10.1161/CIR.0000000000001173

14. Stöger K., Schneeberger D., Kiesebergc P., Holzinger A. (2021) Legal Aspects of Data Cleansing in Medical AI. *Computer Law & Security Review*, vol. 42. DOI: https://doi.org/10.1016/j.clsr.2021.105587

15. Thomas S. at al. (2022) Artificial Intelligence in Vaccine and Drug Design. *Methods in Molecular Biology*, vol. 2410, pp. 131–146. DOI: 10.1007/978-1-0716-1884-4_6

Information about the authors:

B.A. Edidin — Candidate of Sciences (Law), Deputy Director General for Legal Affairs.
A.V. Bunkov — Direction Manager.
K.V. Kochetkova — Candidate of Sciences (Law), Senior Lecturer.

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

The article was submitted to editorial office 10.06.2024; approved after reviewing 28.06.2024; accepted for publication 28.06.2024.