СРАВНИТЕЛЬНОЕ ПРАВО

UDC 341.9, 342, 349

Legal regulation of the transmission of health-related data: Balance of public interests and individual rights in the context of cross-border health care*

I. M. Akulin[1], E. A. Chesnokova[1], U. Genovese[2], R. A. Presnyakov[3], A. E. Pryadko[4]

[1] St. Petersburg State University,
7–9, Universitetskaya nab., St. Petersburg, 199034, Russian Federation
[2] University of Milan,
7, Via Festa del Perdono, Milan, 20122, Italy
[3] Association of Medical Law of St. Petersburg,
29A, 18th line of V. O., St. Petersburg, 199178, Russian Federation
[4] Committee for Social Protection of the Population of the Leningrad Region,
6A, Afonskaya ul., St. Petersburg, 191124, Russian Federation

For citation: Akulin, Igor M., Ekaterina A. Chesnokova, Umberto Genovese, Roman A. Presnyakov, Anastasia E. Pryadko. 2021. "Legal regulation of the transmission of health-related data: Balance of public interests and individual rights in the context of cross-border health care". *Vestnik of Saint Petersburg University. Law* 2: 419–440. https://doi.org/10.21638/spbu14.2021.211

The article provides a comparative analysis of the regulatory and legal regulation for the processing of a special category of personal health data in the European Union and in the Russian Federation in regard to the digitalization of national health systems. Special attention is paid to the legal framework for the transmission of health information at the cross-border level. It is established that within the framework of European and Russian legislation at this stage, in the context of the formation of digital medicine, there is a comparability in the definition of legal mechanisms for the protection of medical data. It is also noted that in the issue of the transfer of personal health data to third countries, both the Russian Federation and the European Union choose the path of strict restrictive regulation and the introduction of a closed list of grounds for overcoming the ban on cross-border transfer. The reasons for this approach to issues of supranational interaction in healthcare are analyzed, as well as the potential risks of inertia of national legislators in this issue. Based on the analysis, the authors propose

* The reported study was funded by the RFBR according to the research project No. 18-29-16215.

a number of amendments and additions to the national legislation on personal data, aimed at simplifying the interaction between jurisdictions on the transfer of confidential medical information. The authors suggest an international agreement on the exchange of medical data in digital format, which potentially should include not only the Russian Federation and the EU states, but also other countries, including Eurasian Economic Union member states, China, and countries of the American continent. The proposed concept is intended to create an opportunity for the formation of a supranational information system in the field of healthcare, which allows for the effective exchange of medical data, taking into account the sovereign interests of the countries participating in the agreement.

Keywords: legislation of the European Union, legislation of the Russian Federation, personal data, medical confidentiality, e-health, data exchange, personal data protection.

1. Introduction

In recent years, we have witnessed and participated in a digital rethinking of almost all fields of social relations. This transformation, on the one hand, facilitates access to information and various services, and on the other hand, fundamentally changes the model of social interaction of people and forms a new kind of public institutions.

One of the most important public institutions undergoing transformation is healthcare. Developed world economies are becoming more and more active in implementing modern digital tools: electronic medical cards, electronic prescriptions, online appointments, etc. Information and telecommunication technologies are becoming a common reality, designed to improve the quality and availability of medical care, to ensure maximum respect for the rights of patients. However, digital transformation in medicine, along with the obvious advantages, creates prerequisites for new risks. Such prerequisites are a rapid increase in the number of information repositories with sensitive data, emergence of new typologies of information, uncontrolled or insufficiently controlled number of persons who can potentially access them, as well as participation of unscrupulous organizations in processing of confidential medical information.

Another factor influencing healthcare transformation is globalization: an increase in migratory activity and in-depth economic integration are the factors driving the familiar national model of healthcare organization to transition to a supranational level and build new structures of interaction between different legal systems. Such convergence of national systems becomes inevitable in the new realities of the digital economy.

The primary link of the supranational model is the cross-border transfer of confidential medical information, which has the same potential risks as the national regulation of "reception" and "transfer" countries. In this regard, it is interesting to summarize the experience of supranational regulation in the European Union (hereinafter — the European Union, the EU, the Union) and the Russian Federation in regard to legal regulation of processing personal data in conditions of economic and political integration of states. In this aspect, the analysis of the relevant Russian and European regulations may be particularly noteworthy for both the EU member states and the Eurasian Economic Union (EAEU) member states.

2. Basic research

2.1. Regulatory and legal framework for personal data within the European Union: providing security during the exchange of confidential medical information

On May 25, 2018 the EU Regulation 2016/679 General Data Protection Regulation (hereinafter — the Regulation, GDPR) entered into force in the European Union[1]. The GDPR is designed to respond to new technological challenges in order to achieve higher legal certainty, harmonization of legal systems and ease the regulation of transferring personal data outside the EU to third jurisdictions. Thus, in accordance with paragraph 10 of the Preamble of the EU Regulation 2016/679 GDPR in order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all member states. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.

This regulation superseded the previous Directive 95/46/EC of the European Parliament and of the Council of the EU[2] which, in fact, is no longer able to fully regulate legal relations between entities in the face of new challenges posed by scientific and technological progress. Yet the objectives and principles of Directive 95/46/EC remain sound (paragraph 9 of the Preamble of the Regulation (EU) 2016/679 GDPR).

Thus, according to the Regulation, the European Parliament and the EU Council pursue an ambitious goal of harmonizing legislation on the protection of personal data in the EU member states and creating a united digital information space throughout the European Union.

The General Data Protection Regulation is an act with a direct effect, its provisions are binding for all EU member states and do not need to be ratified at the level of each EU member state, and the Regulation applies to the European Economic Area. However, the regulation still provides EU member states a free hand to determine requirements, including for the purpose of processing special categories of personal data. Thus, the Regulation does not exclude the legislation of the EU member state, which establishes the circumstances for special processing situations, including a more precise determination of conditions when the personal data will be based on the principle of legality. This fact raises concern for some authors as the provisions of the Regulation to some degree betray the original European idea of harmonization of legislation and may become the reason for the emergence of contrasts between the Regulation and the national laws enacted just because of the need to align national and European regulations (Cataleta, Longo, Natale 2020).

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *EUR-Lex. European Union law.* Accessed July 16, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1563114709430&uri=CELEX:32016R0679.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *EUR-Lex. European Union law.* Accessed July 16, 2019. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

The Regulation establishes the principle of extraterritoriality. Provisions of this act shall be applied if the data processing is related to offering goods or services to natural persons — data subjects located in the Union, regardless of payments (paragraph 23 of the Preamble of the Regulation (EU) 2016/679 GDPR) and when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union, irrespective of the place of establishment of the controller or the person in charge of data processing (paragraph 24 of the Preamble of the Regulation (EU) 2016/679 GDPR). The stated above provisions clearly show a degree of orientation of the European legislator in the first place towards data processing in the field of commercial activity. This is evidenced by the reference to the supply of goods or services, as well as an emphasis on data processing for making decisions related to a natural person located in the EU, or for the analysis or prediction of his/her personal preferences, types of behaviour and attitudes.

At the same time, it should be emphasized that the guarantees of protection provided by the Regulation apply to all natural persons in the EU, regardless of their citizenship, place of registration or place of residence. In paragraphs 23 and 24 cited above, any natural person who is in the Union without indication of their citizenship is considered a data subject. In addition, paragraph 2 of the Preamble of the Regulation states: "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data".

Accordingly, the Regulation for the range of data subjects is applied to all citizens of the Union, persons permanently residing in the territory of the Union, as well as to all individuals in the Union regardless of the purpose and duration of their stay. In this case, the location of the operator processing the data of the above entities does not matter. Therefore, the subject of Regulation also includes cases when citizens and residents of the Russian Federation seek medical care in medical organizations in the territory of the Union.

It should be noted that the Regulation does not provide for a special discipline governing the processing of personal data concerning health, but it does contain a number of provisions related to this category of personal data.

The definition provided in paragraph 15 of article 4 of the Regulation, where the term "data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Paragraph 35 of the Preamble of the Regulation discloses the content of data affecting the state of health, which states that health-related personal data should include all data that is related to the state of health of the data subject and disclose information about the past, current and future physical or psychological state of the data subject's health. This also includes complete information about an individual collected in the course of registration or provision of medical services according to the Directive 2011/24/EU of the European Parliament and of EU Council[3].

[3] In accordance with the provisions of Directive 2011/24/EU of the European Parliament and of the Council of the EU, the information about a natural person collected during registration or the provision of medical services includes: a number, symbol or mark assigned to an individual to uniquely identify that person for health purposes; information obtained from a study or examination of a body part or body material, including genetic data and biological samples; and any information, such as disease, disability, risk

At the same time, it should be noted that the legislator pays special attention to the problem of circulation of data, which to some extent is related to the subject's state of health. In particular, this is evidenced by the specification given in paragraph 35 of the Preamble of the Regulation, which states that all data that is related to the state of health of the data subject and discloses information not only about current but also about the past and future health of the data subject, and the health status concerns both the subject's physical and psychological status.

Further, the definition contains quite a detailed description of the content of the concept. Data concerning health includes:

— information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person;
— a number, symbol, or mark particularly assigned to a natural person to uniquely identify the natural person for health purposes;
— information derived from the testing or examination of a body part or body substance, including from genetic data and biological samples;
— and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

The final provision establishes an open and indicative nature of the list. Thus, the main criterion for classifying data as special is their relevance to information about the physical or psychological state of the subject.

Of particular interest is the fact that in the Regulation the European legislator includes in the "data concerning health" category not only data on examinations and medical services, but also genetic and biometric data. It should be noted that this decision is to some extent a novelty in European norm-setting: the provisions of Directive 95/46/EC preceding the Regulation did not include this category of information in the category on data concerning health.

Health information, as the most sensitive (confidential), belongs to a special category of data and is subject to enhanced protection in terms of guarantees of observance of fundamental human and civil rights and freedoms. However, it is obvious that such close attention to the protection of the data concerning health is also based on the understanding of the importance of providing security of this information in the public interest, and, above all, in order to maintain competitiveness, state security, and national sovereignty. In the European Union, where national borders are more or less non-existent and integration is based on four fundamental European freedoms: freedom of movement of persons, capitals, goods, services, freedom of information flow is a prerequisite for successful integration and implementation of a single policy. In this regard, the Regulation establishes unified rules for circulation of personal information and introduces unified rules for the transfer of information to third parties. It is interesting, however, that the Regulation

of disease, medical history, clinical treatment, or physiological or biomedical condition of the data subject, regardless of the source of the data, for example, it may be obtained from a physician or other medical professional, hospital, medical equipment, or laboratory diagnosis (Accessed February 17, 2021. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:en:PDF).

leaves room for member states, at the legislative level, to provide additional conditions or even restrictions on the processing and transmission of information. At the same time, an extent of readiness of the EU States to make autonomous decisions that strengthen the legal regime for the protection of data concerning health, in our opinion, will be determined by political, social and economic factors.

Thus, the Regulation establishes a basic, minimum level, of personal data protection, which should be provided in all member states, and throughout the EU. Part 1 of article 9 of the Regulation proclaims a general principle prohibiting any processing of data concerning health[4]. However, this prohibition does not apply to a number of situations related to medical services as a whole. In particular, the provisions of § 2 of article 9 of the Regulation allow processing of data concerning health in special public interest, as well as if it is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (sub-paragraphs g, j § 2 of article 9 of the Regulation (EU) 2016/679 GDPR). Processing in the public interest is also allowed when it is necessary in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (sub-paragraph i § 2 of article 9 of the Regulation (EU) 2016/679 GDPR). This provision is particularly significant in terms of European integration. The Regulation establishes the priority of public interests in the field of public healthcare in its cross-border understanding, allowing the processing of personal data, including protection against serious cross-border threats to health, regardless of the will of the personal data subject. It can be assumed that this provision will contribute to the development of a new model of public healthcare that goes beyond national borders and involves more active interaction of all participants in the healthcare system at the EU level.

Processing of health data is also allowed in other cases[5], but the most interesting, in our opinion, are the provisions that lift a ban on processing data concerning health when:

— the data subject has given explicit consent to the processing of personal data for one or more specified purposes, except where Union or member state law provide that the prohibition may not be lifted by the data subject (a);
— processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (c);
— processing relates to personal data which is manifestly made public by the data subject (e).

[4] Part 1 of article 9 of the EU Regulation 2016/679 GDPR specifies that the processing of personal data revealing racial or ethnic origin, political views, religious beliefs or philosophical views, membership in a trade union, as well as the processing of genetic data, biometric data for unambiguous identification of an individual, data relating to the health, sexual life or sexual orientation of an individual, should be prohibited.

[5] In this case, the authors want to point to other cases provided by the provisions of sub-paragraphs b, d, f § 2 of article 9 of the EU Regulation 2016/679 GDPR, as well as the provisions of sub-paragraph h § 3 of article 9 of the EU Regulation 2016/679 GDPR.

This list of exceptions should be considered closed and not subject to broad interpretation. It should be noted, however, that § 4 of the cited article still provides the EU member states with the possibility of national regulation of health data protection. Thus, the EU member states will be able to maintain or introduce additional conditions, including restrictions, regarding the processing of genetic data, biometrical data or health data (Article 4 of the Regulation (EU) 2016/679 GDPR). It seems that this provision should be considered in the sense of possibly further strengthening the protection mechanisms and limitation of the possibilities for personal data processing. For example, as mentioned above, the Regulation establishes a general rule that a ban on the processing of health data can be overcome by the will of the data subject, but it also indicates that the national legislator is allowed to impose a restriction on the ability to dispose of their data.

The basic principles established by the Regulation are the principles of maximum transparency when working with personal data and awareness of the data subject. According to part 1 of article 15 of the Regulation, in the case of processing of personal data belonging to an individual the data subject has the right to access their own personal data, as well as information about the purposes of processing, the category of processed personal data, the recipients to whom the data will be disclosed, the terms of data storage or the criteria used to determine the specified period, the right to request correction or deletion of data ("the right to be forgotten"), restrictions on its processing, or objections, the right to file a complaint with the supervisory authority, the presence of an automated decision-making process, as well as the source of data in case personal data is not received not from the data subject.

Articles 13 and 14 of the Regulation establish a minimum list of information that the controller must provide to the personal data subject.

Articles 33 and 34 regulate the obligation to report data leakage. In accordance with article 33, in case of data leakage the controller should within 72 hours from the time when they have became aware of it, notify the supervisory authority about the leak with a description of the nature of leakage of personal data, indicating where possible the categories and approximate number of data subjects and the categories and approximate number of records of personal data, the possible consequences of the data leakage, as well as measures taken or planned by the controller to eliminate violations and measures to mitigate its possible negative impacts.

Article 34 imposes a duty of the controller to inform the data subject within a reasonable time on the leakage of personal data in case of a potentially high degree of risk for rights and freedoms of individuals. At the same time, as follows from the meaning of the article, if the leakage of personal data can lead to a high degree of risk for rights and freedoms of individuals, the controller shall report the incident to the data subject only if it requires a disproportionate effort, and if the controller resorted to public notification.

In accordance with part 1 of article 12, the above-mentioned information should be provided in a concise, transparent, understandable and easily accessible form that uses clear and simple language. The Regulation establishes a written form of the information document, but it is additionally provided that at the request of the data subject information may be provided verbally on the condition that the identity of the data subject is confirmed in another way.

It seems that these provisions are of particular importance in relation to health data as a special category of personal data.

As mentioned above, the Regulation does not contain a special section establishing rules for processing of data concerning health. The European legislator puts this information into a special category of personal data, and it is subject to protection in accordance with the provisions of the Regulation on personal data and the rules referring to a special category of personal data.

In terms of principles of legality and transparency, the general condition for data processing rests on the consent of the personal data subject. Deviation from this rule is possible only in the cases directly stated in the Regulation. Article 7 of the Regulation establishes conditions for obtaining the consent of the subject. Part 2 of article 7 of the Regulation determines the criterion of awareness and regulates situations when consent to data processing is given in writing in the context of a comprehensive agreement on various issues: the request for consent should be presented in an understandable and easily accessible form in clear and layperson terms in a manner that distinctly distinguishes it from any other circumstances.

Interestingly, the Regulation does not impose on the operator the obligation to obtain consent in writing, but it contains the obligation "to be able to prove that the data subject has agreed to the processing of their personal data" (part 1 of article 7 of the Regulation (EU) 2016/679 GDPR).

Also, part 3 of the cited article establishes the right of the subject at any time to withdraw previously given consent. In that event it is provided, the procedure for consent withdrawal should be as simple as the procedure for granting consent.

It is of interest in the comparative aspect that article 20 of the Regulation contains the right of the subject to receive from the controller copies related to personal data in a structured, universal and machine-readable format, as well as the right of the subject to transfer the data to another controller.

Special categories of personal data are also subject to enhanced protection in the context of an automated decision-making process, including the formation of a profile. Thus, in particular, the general rule establishing the right of the subject of any personal data not to fall within the scope of a decision based solely on automatic processing, including the formation of a profile that creates legal consequences in relation to them or significantly affects them, does not apply if decision-making is permitted by the legislation of the Union or the EU member state, under which the controller falls. It also establishes acceptable measures for protection of the rights, freedoms and legitimate interests of the data subject, as well as, upon the controller's implementation of acceptable measures for the purpose of protection of the rights, freedoms and legitimate interests of the data subject, in cases where there is a direct consent of the data subject, or when this is necessary for conclusion or execution of a contract between the data subject and the data controller.

Thus, in order to overcome the general ban on processing in the context of automated decision-making, including the formation of a profile, it is sufficient, in fact, to introduce an appropriate regulatory framework in the legislation of the EU member state. However, the Regulation significantly limits abilities of the national legislator when it comes to formation of a profile based on data concerning health.

As we can see, at this stage in the EU there is very detailed legal regulation in the field of personal data processing, which forms a primary link for all digital services and systems, as well as for other international systems of interaction that transmit information between individuals and between different jurisdictions.

2.2. Legal regulation of cross-border transfer of medical information in the European Union

As mentioned above, the European Union has taken a number of significant steps over the past few years to intensify the digitalization of healthcare in member states and to create a united European digital circuit system that provides easy access to information and the flow of electronic documents throughout the EU.

On April 25, 2018, European commissioners with reference to the mid-term review on the implementation of the digital single market strategy[6] indicated three areas of development of the united digital circuit:

— citizens' secure access to and sharing of health data across borders;
— better data to advance research, disease prevention and personalised health and care;
— digital tools for citizen empowerment and person-centred care[7].

As a next step, the European Commission presented a number of recommendations to the EU member States on 6 February 2019[8]. In support of the current need for digital healthcare integration, Vice-President Andrus Ansip, in charge of the Digital Single Market, pointed to requests from citizens to allow unhindered and full on-line access to medical information related to them, regardless of which state they are currently in[9].

Currently, the exchange of data and the possibility of forming an electronic prescription for cross-border application is already functioning between such states as Estonia, Finland, Luxembourg, and the Czech Republic. By the end of 2021, 18 additional member states should join[10]. It should be assumed that the speed and completeness of accession to the European information exchange system will be largely dependent on internal social, economic and organizational factors.

The provision of access to electronic databases containing data concerning health within the framework of this system will take place between the EU member States in accordance with the provisions of the GDPR and, in particular, article 9 of the Regulation (Article 9 of the Regulation (EU) 2016/679 of GDPR).

---

[6] Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All. COM/2017/0228 final society. *EUR-Lex European Union law*. Accessed July 18, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A228%3AFIN.

[7] Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society. 2018. *European Commission*. Accessed July 18, 2019. https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering.

[8] Press release. Commission makes it easier for citizens to access health data securely across borders, Brussels (6 February 2019). *European Commission.* Accessed July 10, 2019. http://europa.eu/rapid/press-release_IP-19-842_en.htm.

[9] Ibid.

[10] Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society. 2018. *European Commission.* Accessed July 18, 2019. https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering

At the same time, the EU's goals, inspired by the need to implement the rights of the EU citizens, will be achieved only in part. Thus, it can be assumed that in the coming years the relocation of EU residents outside the EU and the number of cases that involve receiving medical care outside the EU will steadily increase, but the problem of cross-border exchange of health data with third countries outside the EU remains unclear.

According to the analysis of the current European legal framework, in this case the provisions of the Regulations regarding cross-border data transmission should be applied, taking into account the provisions of article 9 of the above-mentioned normative act.

There are particular provisions of the Regulation which cover cross-border data transfer: articles 44–50 of chapter V. Provisions of this chapter are based on the main rule that data protection is transferred together with data. Thus, the provisions of article 44 of Chapter V of the Regulation indicate that all the provisions of this Chapter should be applied to ensure that the level of protection of individuals guaranteed by the Regulation remains unchanged.

According to the provisions of article 45 of Chapter V of the Regulation, cross-border data transfer can take place, first of all, if there is a Decision on Compliance. To this date, such Decisions were taken by the European Commission in respect to the following states: Andorra, Argentina, Australia, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay.

In the absence of a Decision on Compliance, data may be transferred only if the controller or the data processor has provided appropriate safeguards and the data subjects have legally protected rights and effective remedies (Article 46 of the Regulation (EU) 2016/679 of GDPR). Among such safeguards, a special place is held by legally binding corporate rules (Article 47 of the Regulation (EU) 2016/679 of GDPR), including among them binding on each member of a group of enterprises or a group of companies engaged in joint economic activities, including their employees, and which in fact serve as a tool for ensuring the transfer of data from the territory of the EU member state to other states between enterprises of one group. At the same time, according to part 2 of article 15 of the Regulation where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 related to the transfer (Article 15 of the Regulation (EU) 2016/679 of GDPR).

In the absence of the European Commission's Decision on Compliance and in the absence of the above guarantees, cross-border transfer of personal data may take place only if one of the conditions provided for in § 1 article 49 of the Regulations is met. As already mentioned above, with respect to special categories of personal data, the provisions of article 49 of the Regulations shall be applied taking into account the provisions of article 9 of the said regulatory act.

Classic medical justification for partial derogation from the general prohibition on cross-border data transfer lies in obtaining informed consent from the data subject (paragraph a § 2 of article 49 of the Regulation (EU) 2016/679 GDPR). On the same basis, in accordance with paragraph a § 2 of article 9 of the Regulation, the processing of special categories of personal data, which include health data, is permitted. Accordingly, informed consent from the data subject makes it possible to process information about their health and to transmit it outside the state of residence, that is, cross-border. This provision is fully consistent with the modern worldview of the rule of state law, recognizing and protecting

the principle of autonomy of the individual, the priority of an individual's and citizen's freedom of will. However, it should be noted that although the provisions of § 1 of article 49 of the Regulation do not provide for the possibility of a member state to restrict the freedom of expression of will by the data subject, the relevant clause is available in § 2 of article 9 of the Regulation, according to which the processing of health information is possible if the data subject has given direct consent to the processing of personal data for one or more of the established purposes, except for the cases when the legislation of the Union or the EU member state provides that the prohibition specified in § 1 of article 9 of the Regulation cannot be repealed by the data subject.

According to paragraph d § 1 of article 49 of the Regulation, it is possible to derogate from the ban on cross-border data transfer if the transfer is necessary for reasons of public interest. In order to understand the content of the concept "reasons of common interest", one should refer again to article 9 of the Regulation, according to which the processing of special categories of personal data is not prohibited, if it is necessary for reasons of special public interest on the basis of the legislation of the Union or the EU member state, which should be proportionate to the goal and correspond to the essence of the right to data protection and provide acceptable and specific measures to protect the basic rights and interests of the data subject (paragraph g § 2 of article 9 of the Regulation (EU) 2016/679 GDPR). Data processing is also not prohibited in instances of public interest in the field of public health, for example protection against serious cross-border threats to health or to ensure high standards of quality and reliability of medical care and medicines or medical equipment, on the basis of the legislation of the Union or the EU member state that provides acceptable and specific measures to protect the rights and freedoms of the data subject, in particular professional secrecy (paragraph g § 2 of article 9 of the Regulation (EU) 2016/679 GDPR).

Another important reason for the healthcare sector to transfer data to third countries and international organizations in accordance with article 49 of the Regulations is the following: the transfer is necessary to protect the vital interests of the data subject or other persons, if the data subject is physically or legally unable to give consent. In accordance with paragraph c § 2 of article 9 of the Regulation, processing is necessary to protect the vital interests of the data subject or other natural persons, if the data subject is physically or legally unable to provide his consent.

Accordingly, in emergency and urgent care situations in order to save the life or ensure the health of the patient, information can be transferred to a third country without the consent of the data subject, if they are unable to give consent. At the same time, the consent of the guarantor is not required, which greatly speeds up the decision-making process and provides access to information without additional bureaucratic delays.

However, not all issues are fully resolved by the Regulation and other European documents. There are still controversial issues with the procedure in regard to the confirmation of severity of the condition and individuals' inability to express their will. This information must be provided by the person requesting the information. Adequacy and validity of the request should be assessed by the access provider.

In addition, as follows from the meaning of the analyzed regulations, the information should be transmitted exactly to the extent that is required for immediate medical decision making aimed at providing medical care in a particular clinical situation, and it cannot be used for remote prediction and clinical decision-making. Accordingly, the

European operator cannot provide access to the entire electronic medical card of the patient (hereinafter — EMC) upon this request. This is an additional difficulty, since the doctor in this case should clearly formulate what specific data they need (drug allergy, anamnestic information about kidney disease when deciding on a treatment for acute renal failure, etc.). Consequently, the doctor may initially not have a comprehensive view of what information they will need, which will lead to repeated requests, entailing an extremely undesirable time input.

At the same time, it is not unreasonable to assume that in the absence of a clearly regulated procedure of cross-border interaction in the healthcare system, with insufficient technical coordination of the interaction processes as well as in the absence of legal instruments binding the involved persons on both sides of the border to interact and exchange information provided for in paragraph f § 1 of article 49 and paragraph C § 2 of article 9 of the Regulation, an option that allows to derogate from the general ban on the disclosure of medical secrecy, in the vast majority of cases will not be implemented. This may adversely affect the efficiency and promptness of medical care.

On the other hand, in the absence of a relevant international agreement, there is no legal obligation to the requesting person in a foreign country or in an international organization to ensure the transfer of data obtained in the process of providing medical care to the EMC of a patient — a resident of the EU. Possible consequences include the incompleteness of information in the EMC or the absence of clinically relevant information for subsequent observation and treatment. In particular, for the purposes of continuity, information on the performed surgical intervention, on the features of anesthetic aid and resuscitation assistance, on the drugs used, laboratory and instrumental data may be extremely important.

Theoretically, there is still a problem of data compatibility in the case of various standards of formation and storage of digital information.

Thus, the European legislator, being motivated primarily by the aim of observing the realization of human and civil rights and freedoms, adopts a normative act potentially capable of providing a legal basis for protection of rights in the context of new technological challenges and, in particular, in the context of transition to the digital economy. However, it seems that this act does not take into account all the nuances regarding such a socially important sphere of relations as healthcare. The general conditions for cross-border data transfer generally apply to special data categories. Priority is given to the principle of individual autonomy and protection of the fundamental rights to life and health. But the data subject is faced with a choice: to transfer medical data to a third jurisdiction and assume all risks of improper storage or use of this data, or to disagree with the transfer and expose themselves to risks of inadequate medical care. The state of residence does not provide the data subject with the tools to protect data transferred.

In the current political environment, given the large number and diversity of states and international organizations potentially able to engage in interaction and exchange of medical data, it would be premature to assume the possibility of a permanent exchange.

Based on the above, it can be concluded that at this stage the EU has legal regulation and technical capabilities for implementation of cross-border transfer of medical information, which is appropriate in view of modern progressive globalization. Separately, of course, we can note the lack of a single legal basis and the need for the formation of supranational regulation, which will make it possible to create a more dynamic system of

exchange of medical information. However, even the legal and technical tools that exist in the EU presently, to some extent is sufficient to implement its main goal — the transfer of significant medical information.

2.3. Legal regulation of personal data processing in the Russian Federation: cross-border transfer of Private Health Information

Nowadays we see a gradual increase in the flow of tourists between the Russian Federation and the European Union, as well as an increase in the number of Russian citizens who visit the European Union for medical care. Such movement of citizens to foreign jurisdictions may sometimes, on a planned or urgent basis, require information on the state of health of a person in the country of residence. This leads to the issue of cross-border transfer of health data, which is becoming particularly relevant and requires the development of legal mechanisms to facilitate this transfer within the framework of digital healthcare.

In the Russian Federation, the fundamental normative legal act regulating the processing of personal data is the Federal law of 27.07.2006 No. 152-FZ "On personal data" (hereinafter — Law No. 152-FZ)[11].

According to this act, medical data refers to special data (Article 10 of Law No. 152-FZ). Processing of such data, as a general rule, is not allowed except as provided for in part 2 of article 10 of Law No. 152-FZ. The cases of processing specifically medical data are the following:

— existence of consent from the personal data subject to the processing of their data (paragraph 1 part 2 of article 10 of Law No.152-FZ);
— processing of personal data is necessary to protect the life, health or other vital interests of the personal data subject or life, health or other vital interests of other persons and obtainment of the consent of the personal data subject is not possible (paragraph 3 part 2 of article 10 of the Law No. 152-FZ);
— processing of personal data is carried out for medical and preventive purposes, in order to make a medical diagnosis, for provision of medical and medical-social services, provided that the processing of personal data is carried out by a person professionally engaged in medical activities and obliged in accordance with the legislation of the Russian Federation to maintain medical confidentiality (paragraph 4 part 2 of article 10 of Law No. 152-FZ).

Also, the main regulatory legal act regulating judicial relations in the field of public health protection is the Federal law of 21.11.2011 No. 323-FZ "On the basics of public health protection in the Russian Federation" (hereinafter — Law No. 323-FZ), which also reflects the processing of personal data, namely medical data.

According to this law, medical data can be processed either with the consent of the citizen (legal representative), and it should be written, or without their consent, in cases established by the law, for example:

— for the purpose of medical examination and treatment of a citizen who as a result of their condition is not able to express their will, taking into account the

[11] Here and below all references to Russian legal acts are given by "ConsultantPlus". Accessed February 17, 2021. http://www.consultant.ru/document/cons_doc_LAW_61801.

provisions of paragraph 1 of part 9 of article 20 of Law No. 323-FZ (provision of medical assistance in emergency cases) (paragraph 1 part 4 of article 13 of Law No. 323-FZ);
— in case of the threat of infectious diseases spreading, mass poisonings and injuries (paragraph 2 of part 4 of article 13 of Law No. 323-FZ);
— in case of the exchange of information between medical organizations, including those placed in medical information systems, in order to provide medical care, taking into account the requirements of the legislation of the Russian Federation on personal data (paragraph 8 of part 4 of article 13 of Law No. 323-FZ).

At the moment in the Russian Federation, the majority of medical documents are submitted in paper form, however the tendency to further transition to electronic documents management is planned.

As a part of this transition, the Government of the Russian Federation adopted resolution No. 555 of 5 May 2018 "On unified state information system in the field of healthcare", which is a key act that is guiding Russian legislation in the field of healthcare towards digitalization. This act defines the tasks, structure, order of management and access and other provisions related to the unified state information system in the field of healthcare, which should accumulate most of the medical information.

The main document containing data concerning the health of a citizen and other information is the medical card of the patient receiving medical care on an outpatient basis[12]. This document contains private medical information. However, this is not the only medical document that is used in medical organizations. For example, unified forms of medical documentation are used in medical organizations that provide medical care on an outpatient basis, and the procedures for their completion, are approved by the order of the Ministry of healthcare of Russia of 15.12.2014 No. 834н.

The Order of the Ministry of healthcare of Russia of 29.06.2016 No. 425н (hereinafter — the order № 425н) contains an approval of the procedure of familiarization of the patient (their legal representative) with medical documentation, which reflects the patient's state of health.

This order establishes that the patient (their legal representative) who wants to receive data concerning health, should send a written request, which should be answered within 30 days from the date of registration of the written request[13]. The possibility to send a request in electronic form is not clear. In our opinion, the opportunity of sending a request in the form of an electronic document should be provided to the patient or their legal representative, although this does not follow from the literal interpretation of order No. 425н.

At the same time there is quite a long period for giving a response about the possibility or impossibility of familiarization with medical documentation; moreover, in view of

[12] Order of the Ministry of healthcare and social development of the Russian Federation of November 22, 2004 No. 255 "On the procedure for the provision of primary healthcare to citizens entitled to a set of social services". Order of the Ministry of healthcare of the Russian Federation of December 15, 2014 No. 834н "On approval of unified forms of medical documentation used in medical organizations providing medical care in outpatient settings and procedures for their filling".

[13] The Order of the Ministry of healthcare of Russia of 29.06.2016 No. 425н "On approval of the Procedure of familiarization of the patient or his legal representative with medical documentation, reflecting the state of health of the patient".

the period of sending/receiving a request and response, any rapid transfer of information without the use of electronic means of communication is not possible.

Based on the above, in this case there is a gap in the legislation. As a result, it is necessary to supplement order No. 425н with provisions about the possibility of sending a request for provision of medical documents for review in electronic form.

The amendments made to part 5 of article 22 of the Law No. 323-FZ clearly show the orientation of the legislator to digitalization of medical documentation. Thus, in particular, it is established that the request for provision of medical documents (copies) and extracts from them, reflecting the patient's state of health, can be sent in electronic form.

However, to date, the procedure and terms for provision of medical documents (copies) and extracts were not approved by the authorized federal executive body of Russia (Part 5 of article 22 of Law No. 323-FZ). It should be noted that the Order of the Ministry of healthcare and social development of Russia of 02.05.2012 No. 441н approved the procedure for issuing certificates and medical reports.

The Draft Order of the Ministry of healthcare of the Russian Federation "On approval of the procedure and terms for provision of medical documents (copies) and extracts from them"[14]. This Draft provides that a request for information may be sent using an amplified qualified electronic signature or a simple electronic signature through the use of a single system of identification and authentication. The deadline for submission of the requested information is 30 calendar days.

The draft regulatory act that submission of copies of medical documents and extracts from them in the form of electronic documents is allowed only under the following conditions: information about the authorized responsible employee of the medical organization (who sends the specified documents with use of the amplified qualified electronic signature) shall be entered into the federal register of medical employees, on the condition of registration of the relevant medical organizations in the federal register of medical organizations of the unified state information system in the field of healthcare[15].

Also, the draft defines a list of medical documents that are not provided in the original to the patient or their legal representative (only their copy or extracts from them), for example, the history of a child's development, the history of childbirth, the medical card of a dental patient, etc. (paragraph 4 of the Project).

Thus, the citizen (their legal representative) has the right to receive duly certified medical documents (both in paper and electronic form), copies of medical documents or extracts from them in the manner prescribed by the law.

Nevertheless, we would like to emphasize the rather long-term process of providing the required information (its request, response to the request and actual receipt); moreover, there are nuances in the transfer of information in electronic form. We would also like to note that the grounds for refusal to provide documents are not defined, thus, the powers of the medical organization are quite broad. For example, a medical organization has the right to refuse to provide medical information if it has doubts on authenticity of the signature of the personal data subject[16].

---

[14] Draft Order of the Ministry of healthcare of the Russian Federation "On approval of the procedure and terms for provision of medical documents (copies) and extracts from them".

[15] Resolution of the Government of the Russian Federation of May 5, 2018 No. 555 "On the unified state information system in the field of healthcare".

[16] The Ruling on the appeal of the Investigative committee for civil cases of the Krasnoyarsk regional

Therefore, we believe that the legal act should establish a specific list of grounds for refusal to provide medical information, since in this case, the medical organization is given an opportunity to make a decision at its discretion.

As already mentioned, in the Russian Federation most medical data is presented in paper form, but there is a trend towards further digitalization of the data. In particular, the Russian Federation has adopted and implemented GOST R 52636-2006 Electronic medical records. General provisions (amended)[17].

This document defines such concepts as personal medical record, electronic medical history, electronic personal medical record, electronic medical archive.

It defines the life cycle (maintenance and subsequent archiving) of electronic personal health records (further — EPHR). Regarding the transfer of medical record copies using electronic communication channels, it states that this action is allowed, however the "Security policy" of the medical organization should state the following:

— the procedure for transmission of electronic copies of EPHR to patients, the method of registration of transfer of copies and notification of patients about the rules of confidentiality of personal medical data; the recommendation says that it is necessary to develop a checklist for patients on how to use electronic copies of EPHR;
— the procedure for transfer of electronic copies of EPHR to independent and parent organizations, requests for copies, the method of registration of transfer of copies and documents being the basis for such transfer.

It is established that a cover letter to the document containing EPHR should be instructions on how to access EPHR.

Thus, most of the information that should be stated in the "Security policy" of the medical organization is left to the discretion of the organization. This results in a lack of uniform rules and, in some organizations, a complete lack of them.

In our opinion, the "Standard security policy" of a medical organization should be developed, which should reflect key stages of medical data transmission.

Transition to electronic document management, of course, simplifies the process of personal data processing. However, in practice, there are often difficulties with the transfer of medical data to medical organizations abroad.

Article 12 of Law 152-FZ establishes that cross-border transfer of personal data is possible if:

— the parties are parties to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[18] — ratification of this Convention by the parties involved in the personal data processing;
— the state where it is planned to transfer personal data to provides an adequate protection of the rights of personal data subjects, which is carried out in accordance with Law 152-FZ.

What is the difficulty?

court of October 1, 2014, case No. 33-9443/2014.

[17] GOST R 52636-2006 Electronic medical history. General provisions (amended). Accessed June 2, 2019. http://docs.cntd.ru/document/1200048924.

[18] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Made in Strasbourg on 28.01.1981). 2014. April. *Bulletin of international treaties* 4: 1–9.

First, prior to the transfer of personal data, the operator (the person transferring personal data) must ensure that the rights of personal data subjects are adequately protected in the foreign state to which the transfer of personal data is planned.

The procedure for verification of adequate protection of the rights of personal data subjects remains uncertain.

On the one hand, accession to the Convention on protection of natural persons at the automated processing of personal data essentially means that the state provides data protection from a formal point of view.

On the other hand, the list of foreign states that are not parties to the Convention of the Council of Europe on the protection of individuals in the automated processing of personal data, but which provide adequate protection of the rights of personal data subjects, is approved by the decree of Roskomnadzor dated 15.03.2013 No. 274[19].

According to the explanations of Roskomnadzor, for the purpose of inclusion of the state into this list it is necessary to comply with the following conditions in a foreign country: presence of a normative legal act regulating the sphere of personal data, the presence of an authorized body for protection of the rights of personal data subjects and a system of sanctions provided for violation of the legal requirements in this field[20].

Thus, before the transfer of personal data, the operator should make sure that the country to which the transfer of personal data is planned is included in these two lists.

Part 4 of article 12 of Law 152-FZ defines the cases when the transfer of personal data can also be carried out to other persons who do not provide adequate protection of personal data. In particular, such a transfer is possible with the written consent of the personal data subject, performance of the contract to which the personal data subject is a party, as well as for the protection of life, health and other vital interests of personal data subjects, in case of the impossibility of obtaining consent in writing.

Some authors say that there is a problem of insecurity of the rights of the personal data subject when sending their personal data to a state in which there is no adequate protection of personal data, if the subject is a party to the contract (Kucherenko 2009). This is explained by the fact that according to article 430 of the Civil code, the contract can be concluded for a third party (personal data subject).

We would also like to consider such a case of processing of special personal data provided for in paragraph 4 of part 2 of article 10 of Law No. 152-FZ as the processing of personal data for medical and preventive purposes. Data is processed in order to establish a medical diagnosis, the provision of medical and medical and social services, provided that the processing of personal data is carried out by a person professionally engaged in medical activities and obliged in accordance with the legislation of the Russian Federation to maintain medical secrecy.

In this case, special requirements for the person processing personal data are established: professional medical activity and obligation to maintain medical secrecy in accordance with the legislation of the Russian Federation. At the same time, article 12 of

[19] Decree of Roskomnadzor (Federal Service for Supervision of Communication, Information Technology and Mass Media) of 15.03.2013 No. 274 "On approval of the list of the foreign states which are not parties to the Convention of the Council of Europe on protection of physical persons at the automated processing of personal data and providing adequate protection of the rights of personal data subjects".

[20] "Updated list of countries providing adequate protection of the rights of personal data subjects". 2019. *Roskomnadzor.* Accessed June 8, 2019. https://rkn.gov.ru/news/rsoc/news65616.htm. (In Russian)

Law No. 323-FZ establishes a fairly wide list of persons who are obliged to keep medical confidentiality: these are the persons, who received the information at training, execution of labor duties, office duties, job duties and other responsibilities. However, Law No. 323-FZ regulates legal relations arising in the sphere of public health protection in the Russian Federation. In the vast majority of countries, persons engaged in professional medical activities are obliged by their national legislation to maintain medical secrecy. We believe that the rules provided for in paragraph 4 of part 2 of article 10 of Law No. 152-FZ apply only to the primary processing of personal data, which is carried out by a Russian medical organization, since the internal legislation of the state operates exclusively in the territory of this state and does not apply to non-residents of the state who are in the territory of another state.

Thus, there are no special restrictions on the cross-border transfer of personal data (including medical data) in Law 152-FZ; in the case of written consent or a contract to which the personal data subject is a party, personal data may be sent to a foreign state that does not provide protection of personal data (there are no advantages and no simplified procedure for transferring data to countries that provide adequate protection of personal data). That is, in fact, the transfer of personal data is allowed to any country of the world.

Second, in any case, the operator is obliged to notify the body authorized for the protection of the rights of personal data subjects (Roskomnadzor) on the cross-border transfer of personal data (Article 22 of Law 152-FZ).

In paragraph 3.1.11 of the Order of Roskomnadzor dated 30.05.2017 No. 94 "On approval of methodological recommendations on notification of the authorized body on the beginning of processing of personal data and on amendments to the previously submitted information", it is stated that the notification on processing of personal data should indicate the specific state to which the transfer of personal data will be carried out.

In addition to notifying Roskomnadzor, the operator is also required to notify the subject of personal data about such a transfer.

Third, also, in the case of transferring personal data via the Internet, the operator can use only encryption facilities certified by the Russian Federal security service (and data of encryption facilities should only be of domestic production, there are features of the turnover of such means, which do not simplify the process of transferring personal data). The operator is obliged to provide protection to the data transmission channel. That is, for example, the transfer of medical personal data via e-mail without the use of cryptographic protection of information will be a fact of disclosure of personal data and a violation of the requirements for personal data protection.

Fourth, the procedure for cross-border transfer of personal data should also be stated in the local legal acts of the data operator, as mentioned earlier.

The following provision set out in the work entitled "Safety of storage and transfer of medical (personal) data in the multilateral exchange of medical information" for the "International Space Station" program is particularly interesting: "one of the forms of regulation of cross-border transfer of personal data is an existence of a written agreement containing the requirements agreed by the parties for the purpose of protection of personal data at their cross-border transfer" (Shulenin, Skorokhodov, Kantemirova 2012). The presence of such a document would significantly simplify the procedure of cross-border transfer of personal data, but such agreements only seem appropriate in the presence of personalized and permanent participants of cross-border transfer of personal data. In our

case, a medical organization often acts as an intermediary between a patient and a foreign medical organization.

Thus, the mechanism of cross-border transfer of personal data is quite complicated, and yet it should protect the transferred personal data from intruders.

In part, this issue was also addressed in a number of other works (Serafimov 2018; Sokolova 2019; Kheifets, Kheifets 2020; Hartley 2014; Horspool, Humphreys, Wells-Greco 2018).

Also, after adoption of the Federal law of 21.07.2014 No. 242-FZ "On amendments to certain legislative acts of the Russian Federation in terms of clarifying the procedure for processing of personal data in information and telecommunication networks" (hereinafter — Law No. 242-FZ), one of the topical issues was the question of the possibility of cross-border transfer of personal data, since the above-mentioned law establishes the obligation of the data operator to process personal data using databases located on the territory of the Russian Federation (and cross-border data transfer involves the transfer of data to the territory of a foreign state, whose databases are not in Russia).

An answer to this question was provided in the explanations of the Ministry of digital development, communications and mass media of the Russian Federation[21], which states that the adoption of Law No. 242-FZ in no way affected the cross-border transfer of data, since personal data before the transfer to a foreign person is initially entered into a database located on the territory of Russia ("primary database"), and then transferred to a foreign person for inclusion into a "secondary database".

As already mentioned, the main international document containing legally binding rules for Russia in the field of cross-border transfer of personal data is the Convention on the protection of individuals in the automated processing of personal data (hereinafter — the Convention).

Article 14 of the Convention is noteworthy as it states that if a person is a citizen of another state, permanently residing in the territory of a foreign state, they have the right to request the required information through the authorized body in the state in which he lives, from the state of which he is a citizen. The body to which the request for such information is sent must assist in obtaining it (refusal is only possible in the circumstances defined in article 16 of the Convention, for example, if the execution of the request would violate the sovereignty, security of the state). Article 17 stipulates that the forms, procedures and languages used in cross-border transfers shall be determined directly between the states concerned. However, such agreements between the Russian Federation and another state were not found during the analysis. At the same time, the status of persons who temporarily reside in the territory of a foreign state are not defined in the Convention.

It should be noted that there is a tendency to develop international legal acts by participants of various international associations.

The Resolution of the Interparliamentary Assembly of Member Nations of the Commonwealth of Independent States (hereinafter — CIS) of November 25, 2016 No. 45-13 "On the model law 'On cross-border information exchange of electronic documents'" (hereinafter — the model law) serves as the basis for legal support in the cross-border exchange of information by CIS members and the harmonization of national legislation (Part 4 of article 1 of the model law). Part 2 of article 3 of the model law defines that the

[21] Processing and storage of personal data in the Russian Federation. Amendments since September 1, 2015. Accessed June 9, 2019. https://digital.gov.ru/ru/personaldata.

CIS Member Nations create an interstate coordinating body, which defines the rules and requirements for documentation in cross-border information exchange. At the same time, part 3 of article 4 of the model law states that the cross-border transfer of personal data is regulated by the national legislation of the states. This document establishes the need to develop a cross-border space of trust (Article 11 of the model law).

Similar rules on the creation of a cross-border space of trust are stated in part 1 of article 23 of the Treaty on Eurasian Economic Union[22] — another international organization.

In its turn, the requirements for creation, development and operation of the cross-border space of trust are determined by the decision of the Council of the Eurasian Economic Commission dated 05.12.2018 No. 96 "On the requirements for creation, development and operation of the cross-border space of trust".

Thus, there is an active development of the regulatory framework for cross-border data transfer, including the transfer of medical data. However, only basic documents that define the main provisions of cross-border data transmission are being created, while there is no detailed regulation in specific areas of public life.

The experience of another international association — the European Union — also seems relevant. In June 2019, the first session of the trans-border transfer of medical data was held, information about this was published on the website of the European Commission[23]. Information provided states that now a doctor from Luxembourg can obtain the electronic medical history of a traveler who came from the Czech Republic, in particular about allergies, surgical operations, etc. This is information that may be needed in case emergency medical care and it is now available in electronic form. Also, in the framework of eHealth there is a system of the electronic exchange of prescriptions, for example, now citizens of the Republic of Finland can get medicines from Croatia that they were prescribed by a Finnish doctor.

In the Russian Federation and partner countries (CIS, Eurasian Union), the specified legal framework is just beginning to be developed. Work on this is of a general nature and not divided into certain areas (which is likely to happen in the future).

In view of the dynamic development of the legal framework of the Russian Federation in terms of digitalization of healthcare, we believe that after the completion of the formation of a state system in the field of healthcare, it will be necessary to amend the decree of the Government of the Russian Federation of May 5, 2018 No. 555 "On the unified state information system in the field of healthcare" in order to regulate the implementation of cross-border transfer of medical data.

The active legal regulation of cross-border data transmission and accompanying development and creation of information systems will allow for inter-state data transmission, fundamentally transform social institutions, simplify many procedures for ordinary citizens, which will provide better health services, and ultimately lead to better lives for many people, regardless of their place of residence and citizenship.

[22] Treaty on Eurasian Economic Union (Signed in Astana on 29.05.2014). Accessed June 9, 2019. https://www.un.org/en/ga/sixth/70/docs/treaty_on_eeu.pdf.

[23] "Daily News 21/06/2019". 2019. *European Commission.* Accessed June 23, 2019. http://europa.eu/rapid/press-release_MEX-19-3351_en.htm.

3. Conclusions

As a result of the analysis, it can be concluded that within the framework of European and Russian legislation at this stage there is comparability in the protection of medical data in the context of digital medicine. Also, there are certain differences in approaches to the regulation of rights of health data subjects in the framework of the national e-health systems. However, these differences are not final as the Russian legal regulation is still in the stage of dynamic formation, and its final form is unknown at the moment. Nevertheless, the Russian legislator has already determined the vector for development of legal regulation, and it is unlikely to change.

In regard to legal regulation of health data transfer to third countries, both the Russian Federation and the European Union have chosen the way of severe restrictive regulation and introduction of a closed list of grounds for overcoming the ban on cross-border transfer. The restrictive approach can be justified both by the public interest and the need to ensure the observance of individual rights of citizens to privacy, while the ratio of individualization of situations where the transfer of medical data is permissible, as a rule, lies in significant public interest that can prevail over individual risks of violation of the rights of data subjects. However, both in the EU and in the Russian Federation data transmission is legally permitted in cases where it is necessary to save the life or health of individuals, as well as in situations where the data subjects themselves give informed consent to their transfer. At this stage the states permitting the transfer decline all responsibility for what happens further, both with respect to the de facto execution of the data exchange procedure and its timing, and with respect to the further handling of the transferred data if the transfer, as such, has taken place.

In this regard, it seems timely and extremely urgent to provide for the possibility of concluding an international agreement on the exchange of medical data in digital format, the participants of which potentially should be, first of all, the EU member states, the EAEU, China, and the countries of the American continent.

The supranational system formed within the framework of this agreement should solve the following tasks:

— ensure compatibility of national and international digital healthcare systems;
— provide legal and technical mechanisms for transmission and protection of health data;
— provide conditions for international cooperation on issues of electronic data security and combating cybercrime.

At the same time, the basis for the obligation to request and provide access to information, respectively, should be the principles of the maximum enforcement of the right to life and health, the right to private life, the principle of individual autonomy, as well as public interests in the field of public health, such as the threat of infectious diseases spreading, etc.

Accordingly, the proposed supranational system should essentially represent a legal and technical basis covering the maximum possible geographical space. In other words, the system should be a permanent mechanism in stand-by mode, whose individual links should be included and interact only on clearly defined grounds:

— threat to the life or health of the data subject or other persons if the consent of the data subject cannot be obtained;

— informed consent of the data subject or its representative;
— public interests in the field of public health in the threat of infectious diseases spreading, mass poisoning and damage;
— international cooperation in the fight against crime;
— additional grounds, in our view, could be included within the framework of bilateral agreements between the states and organizations.

Also, in light of potential expansion of the number of states that accede to the proposed agreement and, as a consequence, the potential for a significant difference in the constitutional structure of the states concerned and in the different approaches to the application of international normative regulation, the proposed agreement on international electronic cooperation in the field of healthcare should provide for provisions binding the signatory and acceding states to implement the provisions of the agreement into national legislation. The agreement should also provide in national systems of law the rules of legal responsibility of natural and legal persons for violation of the provisions of the proposed agreement.

References

Cataleta, Anna, Alessandro Longo, Raffaella Natale. 2020. "GDPR, tutto ciò che c'è da sapere per essere in regola". *Digital 360.* Accessed May 26, 2018. https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati.

Hartley, Trevor. 2014. *The Foundations of European Union Law: An Introduction to the Constitutional and Administrative Law of European Union.* New York, Oxford University Press.

Horspool, Margot, Matthew Humphreys, Michael Wells-Greco. 2018. *European Union Law.* 10th ed. Oxford, Oxford University Press.

Kheifets, Nikolay E., Evgeny N. Kheifets. 2020. "Human rights in the aspect of doctor-patient relations in the era of e-health. Part 1. European practice of legal regulation of relations related to the handling of special personal data". *Voprosy organizatsii i informatizatsii zdravookhraneniia* 1 (102): 10–29. (In Russian)

Kucherenko, Anna V. 2009. "On guarantees of the rights of subjects at implementation of cross-border transfer of personal data". *Information law* 3: 14–17. (In Russian)

Serafimov, Victor. 2018. "Extraterritorial application of the EU general DATA protection regulation". *Kutafin University Law Review* 5 (2) (10): 469–479. https://doi.org/10.17803/2313-5395.2018.2.10.469–479.

Shulenin, Anatoly P., Skorokhodov Anton V., Kantemirova Ekaterina V. 2012. "Security storage and transmission of medical (personal) data for the multilateral exchange of medical information in frame of the program 'The International Space Station'". *Trudy 14-i Vserossiiskoi nauchnoi konferentsii "Elektronnye biblioteki: perspektivnye metody i tekhnologii, elektronnye kollektsii" — RCDL-2012, Pereslavl'-Zalesskii, Rossiia, 15–18 oktiabria 2012 g.* Accessed June 6, 2019. http://ceur-ws.org/Vol-934/paper50.pdf. (In Russian)

Sokolova, Marianna E. 2019. "Between business interests and security: American it giants and personal data protection". *Rossiia i Amerika v XXI veke* 2: 6. https://doi.org/10.18254/S207054760006015-3. (In Russian)

Received: November 12, 2020
Accepted: March 15, 2021

Authors' information:

Igor M. Akulin — Dr. Sci. in Medicine, Professor; akulinim@yandex.ru
Ekaterina A. Chesnokova — PhD in Medicine, Associate Professor; e.chesnokova.spbu@mail.ru
Umberto Genovese — MD, Associate Professor; umberto.genovese@unimi.it
Roman A. Presnyakov — LLM; r.presnyakov@inbox.ru
Anastasia E. Pryadko — LLM; anastasiis.pr@yandex.ru