DOI: https://doi.org/10.30525/2256-0742/2021-7-5-228-234

ECONOMIC POLICY OF THE STATE IN CONDITIONS OF INFORMATIZATION OF HEALTH CARE IN UKRAINE AS AN INTEGRAL PART OF THE SOCIAL SPHERE

Tetiana Arifkhodzhaieva[1], Iryna Ponomarenko[2]

Abstract. *The purpose of the article* is to analyze domestic and international legal norms on the protection of medical information in order to improve the system of national legislation in the field of health care. *The methodological basis* of this study is a system of methods, the set of which is determined by the purpose and features of the study: dialectical, systemic, system-structural, analytical-synthetic, comparative-legal methods of analysis of domestic and international legal regulation of economic policy of the state in the conditions of informatization of health care of Ukraine. It argues that Ukraine, seeking to integrate into the European space and building its own strategy of economic development, must be clearly aware of both its capabilities and external factors of influence. The choice of possible alternatives is too complex a task, but the leading idea of socio-economic policy should remain the desire to ensure sustainable economic development of the country. In particular, the following is analyzed: recent international and domestic normative acts regulating state economic policy activities in the field of health care informatization in Ukraine: in particular, General Data Protection Regulation of the European Union (GDPR), CMS Interoperability and Patient Access Final Rule, ONC's Cure Act Final Rule, Order of functioning of the electronic health care system of Ukraine; materials of judicial practice, including materials of cases of the European Court of Human Rights, the results of sociological research. A comparative analysis of the GDPR and the Health Insurance Portability and Accountability Act (HIPAA) was conducted. The main problematic issues of state economic policy in the context of health informatization in Ukraine are highlighted. Compared to previous regulations governing medical data, the GDPR pays much more attention to the implementation of new requirements that have arisen due to the growing digitalization of healthcare, and therefore may contribute to strengthening their protection. *Results*. It is theoretically substantiated that quality medical reform is possible only with the introduction of modern methods of informatization and, consequently, information protection. As the analysis has shown, currently in Ukraine the legal system providing information protection in the medical sphere needs immediate improvement. This requires: systematizing and codifying national legislation in accordance with European legal norms and international law; developing a comprehensive legislative act, which would regulate the collection, protection and transition of medical information at the legislative level, following the example of GDPR (for structuring the medical information system, ensuring mandatory certification for information protection, development of cryptography/encryption technologies, delimitation of rights of access to information for medical workers, ensuring access to information with mandatory use of electronic signature, medical workers need to take short courses and register with information security specialists (defined access rights and the ability to change the level of access, provide input for identification and authentication), correcting data and entering new information is carried out with a confirmation of electronic signature, develop an algorithm for transferring information between medical institutions).

Key words: economic, medical reform, informatization, information protection, codification, information-communication technologies.

JEL Classification: G14, D83

Corresponding author:
[1] Interregional Academy of Personnel Management, Ukraine.
E-mail: ariftabo@ukr.net
ORCID: https://orcid.org/0000-0002-1827-1699
[2] National Academy of Security Service of Ukraine, Ukraine.
E-mail: Ponomarenkoirin@gmail.com
ORCID: https://orcid.org/0000-0003-1434-4552

1. Introduction

Stable economic development of the state and society is impossible without the existence of both socially protected and socially oriented population of the country. The relevance of socially-oriented administrative and legal regulation of the country is increasing in the context of the economic crisis, the pandemic coronavirus, military actions in the East, which in general has a negative impact on the welfare of the population both today and in the near future. The socialization of the Ukrainian economy involves filling all reforms with social content, activating the social role of the state, working out the mechanism of interaction between the state and society in the social sphere, ensuring decent living and working conditions, increasing the well-being of citizens (Obervan, 2012). The highest social value is human life and health, information about the state of which is an important component of the social characteristics of a citizen as a participant in all social relations (Constitution of Ukraine, 1996). Health care is a complex socio-economic system that provides organizational and socio-economic relationships that are formed in the process of meeting the needs of the population for medical services. According to A. G. Akhlamov and N. L. Kusyk: "From an economic perspective, only adequate health care improves the quality of human capital by increasing a person's ability to work productively" (Akhlamov, Kusik, 2011). Protection of human rights, including the right to information, is a fundamental constitutional right. Ensuring human rights, including the right to medical information, is what determines both the level of democracy of the state itself and the level of integration of national law into the world community, the compliance of the law with international legal standards (Martsenyuk, 2018).

Due to the significant changes taking place in the course of medical reform, there is an urgent need to amend the current legislation with regard to the further implementation of the electronic health care system. After all, the quality of information management methods determines the effectiveness of first aid and further patient treatment. Unfortunately, today the exchange of personal health records between health care providers, health information networks, health care providers and patients is complicated by the problematic economic, technical and legal protection of so-called "sensitive personal data", which are subject to heightened protection requirements under relevant laws. This issue, as K. Yu. Tereshko rightly pointed out, is a sensitive, human-centered one, since it is particularly vulnerable, as the European Court of Human Rights has repeatedly emphasized: "Protection of personal information (especially medical information) is fundamental to the right to respect for private and family life. Respecting the confidentiality of medical information is a basic principle of the legal system of all state parties to the Convention" (the case "M.S. v. Sweden", 1997; Tereshko, 2019).

Issues of functioning of social economic policy in the conditions of informatization of health care of Ukraine were studied by both domestic and foreign scientists, in particular O. Evseeva, J. Zhalilo, A. Chukhno, O. Stefanyshyn, L. Shevchuk, O. Novikova, E. Libanova, V. Akopov, A. Andriychuk, H. Blinova, N. Bolotina, T. Hurs'ka, M. Maleina, O. Martsenyuk, A. Marushchak, I. Seniuta, S. Stetsenko, V. Soloviov, K. Tereshko, O. Tykhomyrov, etc. However, according to the analysis of European and domestic legislation, scientific research in the field, case law, including the European Court of Human Rights, in connection with recent changes in legislation, they have partially lost relevance, which led to the choice of the topic of research.

The methodological basis of this study is a system of methods, a set of which is due to the purpose and peculiarities of the study. Dialectical method allowed to identify trends in the development of socio-economic policy in terms of informatization of health care in Ukraine and formulate proposals to improve domestic legislation in this direction. The systematic method and the method of analysis were used to identify the relationship between the problems of development of information law in the medical sphere and the essence of socio-economic processes. The combination of methods of system-structural analysis and analytical-synthetic method allowed to propose a new model of the information industry and the subject of legal regulation. Using the comparative legal method the analysis of domestic and international legal framework for the regulation of information security in the medical sphere was carried out. Proposals for improving national legislation were also given.

2. Research results

State social policy is an integral part of the economic sphere, and the direction of its implementation depends on the state economy. Social policy, according to A. A. Kochetkova, "A system of economic relations in which the state provides each member of society with legal guarantees of a decent standard of living..." (Kochetkov, 2005). Health economics studies the socio-economic patterns of formation and use of material, labor and financial resources aimed at improving the health care system and medico-social support measures to improve public health (Akhlamov, Kusik, 2011). Improving public health and improving the quality and efficiency of medical services in the context of digitalization are the main objectives of health care.

An analysis of "...incidents in the first half of 2020 showed that the healthcare industry has failed to protect the main artifact of the digital age – citizens' personal data, including medical records. The main channel of information leakage (e.g., information related to the coronavirus pandemic) was the Web. In 64.2% of cases around the world personal data was spread in the form of lists – documents, reports, fragments of records, in 35.8% of cases the leak occurred as a result of hacking into data storage, illegitimate access to data, accidental disclosure due to improper server settings or application errors" (COVID-19, 2020).

According to the Info Watch Group Center of Expertise, which investigated COVID-19-related medical information leaks, there were 72 cases of leaks in the first half of 2020 alone. For example, the personal and medical records of 16 million coronavirus patients in Brazil were exposed to the public because a hospital employee accidentally posted a spreadsheet on GitHub with usernames, passwords, and keys to confidential government systems. The information was eventually removed from GitHub, and government officials changed passwords and revoked access keys to secure their systems (COVID-19, 2020). Similar leaks have occurred in Germany, Wales, New Zealand, India, and other countries. Even worse, according to Interdust analysts, about 85% of COVID-19 contact tracing apps still leak data. As can be seen, the coronavirus pandemic has highlighted a number of problematic issues related to information security in the medical field.

At the same time, according to a Black Book Market Research LLC survey of more than 3,600 respondents (security professionals, providers) in late 2020, "spending on cybersecurity by European healthcare facilities has been trending downward since 2019, and 92% of healthcare facilities have no security staff at all" (Rule of interaction, 2020).

3. European Union General Data Protection Regulation

In May 2018, a truly "landmark" document in the direction of data protection came into force. In the medical field, the European Union General Data Protection Regulation (GDPR) was adopted, replacing previous data protection laws in the EU. Health information is defined in this document as a "special category" of personal data that is considered "sensitive" in nature, and therefore has a higher level of processing security (General regulation for the acquisition of personal tributes from the European Union (GDPR), 2018). GDPR involves a reformatting in terms of control and ownership of medical records. These are moving from doctors, scientists, hospitals, and health care providers to patients. Patients are now required to consent to the use of their medical data and can revoke it if necessary.

Thus, compared to previous health data protection rules, the GDPR is much more focused on meeting the new requirements that have arisen with the increasing digitalization of health care, and can therefore strengthen their protection. Personal data must be processed in accordance with the following data protection principles: processed lawfully, fairly and transparently; collected for a legitimate purpose; adequate, relevant and limited by necessity; accurate; kept for as long as necessary; security, integrity and confidentiality ensured (European Union General Data Receipt Regulation (GDPR), 2018). The GDPR sets higher standards for informed consent and notification obligations (Art. 7), strengthens the protection of the right of access to personal health data. It is worth noting the fact that data controllers inform the supervisory authority within 72 hours if personal data are leaked (art. 33, 34), and they must inform patients in case of a data security breach (General regulation for the acquisition of personal tributes from the European Union (GDPR), 2018). Therefore, the GDPR clearly states that organizations must be accountable for the personal data they collect. This is ensured by conducting a legal audit to assess not only what kind of personal data has been collected, but also how it is protected.

As can be seen, the GDPR does deserve attention. But despite the fact that it has been in force for two years now, some problematic issues still arise. For example, for February 2021 alone: a) Sky Med International is accused of failing to take adequate measures to ensure the security of subscribers' personal information on membership emergency travel plans. As a result, the company left an unsecured database containing 130,000 member records (the unsecured database contained members' personal information stored in plain text, such as names, dates of birth, home address, medical records and member account numbers). In addition, the FTC claimed that Sky Med misled consumers by stamping "HIPAA Compliance" on every page of its website, giving the false impression that its privacy policy had been revised to comply with the Health Insurance Portability and Accountability Act (HIPAA) security and privacy requirements (FTC Gives final, 2021); b) in Poland, a fine (85,000 PLN) was imposed on a private entrepreneur, a provider of medical services. In particular, according to the instructions of the Polish Personal Data Protection Authority, the private entrepreneur was obliged to inform his patients about the breach of their personal data and to give them recommendations to minimize the possible negative consequences of the incident. Given that the administrator did not do that, in accordance with Art. 58 Sec. 2 of the GDPR, an administrative

fine was imposed on him (The first penalty for failure to comply with the order of the administrative decision, 2018).

4. Health Insurance Portability and Accountability Act (HIPAA)

It should be noted that in 1996, the Health Insurance Portability and Accountability Act, or HIPAA, was enacted in the United States of America (USA) to legislate for the protection of health information, with the primary purpose of regulating health insurance portability and accountability and setting standards for protecting patients' medical records and personal health information (Health Insurance Portability and Accountability Act, 1996). HIPAA allows the use of the "Necessary Minimum" rule (U.S. Department of Health & Human Services, 2020) when developing systems that meet all privacy requirements, i.e., the system must report all necessary efforts to use, request or disclose only the information that is minimally necessary to achieve the goal. HIPAA-compliant applications are considered to be the most secure around the world.

The main difference between the GDPR and HIPAA is that HIPAA applies only to the collection and processing of medical personal data. It directly applies to a specific range of people who have access to this group of data. In addition, it is very important that under HIPAA you can disclose PHI (health information that identifies an individual – names, phone numbers, addresses, dates of birth, social security numbers, payment information, medical test results, medical records, photographic images, x-rays, etc.). (Fact sheet on interoperability and patient access, 2020) for the purpose of treatment without prior patient consent, whereas under the GDPR the primary basis for the disclosure of medical data is the patient's explicit consent (provided that the patient is capable of knowingly giving such consent). In addition, HIPAA, unlike GDPR, does not provide for a patient's right to request that his or her medical records be expunged from the medical facility.

Full user privacy in compliance with HIPAA is ensured by the Curogram platform (a unique development in telemedicine that supports video communication, two-way text messaging via smartphone and works directly with any electronic medical record system). Curogram helps healthcare providers automate workflows, streamline interaction between doctors and nurses, better coordinate patient care, and find and connect with other healthcare providers faster (Curogram, 2019). It is important to emphasize that the objects of protection in a medical institution's information system are: information in databases (DB) of database management systems (DBMS); file server resources of a medical institution; DB backups of DBMS and archival copies of file server resources; information of the manager's operating system, DBMS, automated workstation (AWS) of the medical information system (MIS) administrator and information security (IS) administrator; technological process of collection, processing, storage and transfer of information in MIS; hardware and software complex that ensures MIS operation (secure multilateral computing, 2020). Any user of the healthcare facility who has access to the MIS is morally, administratively and criminally responsible for the confidentiality of the information he or she enters, uses, or transmits to other users.

It's worth emphasizing that in February 2021, two pieces of legislation will go into effect in the United States to work with HIPAA – the CMS Interoperability and Patient Access Final Rule (implementation and support of secure and interface-based application programming that allows patients to easily access their applications. The CMS rule also requires Medicare and Medicaid providers to send electronic notifications of a patient's admission, discharge, or transfer to another health care facility to the community provider or practitioner) (Achieving confidentiality in electronic health records using cloud systems, 2020) and ONC's Cure Act Final Rule (applies to health IT systems as well as health care providers, health information exchanges, and health information networks used by such systems. The rule requires all systems to implement standardized APIs so that patients and their health care providers can easily retrieve electronic health information using smartphone apps. The central component of the rule is the blockchain provisions that prohibit actions that impede access and exchange of EHI, with some exceptions for privacy and security) (Blockchain Technology Analysis, 2020). The main purpose of these documents is to make it easier for patients to access their medical records, while respecting appropriate security and confidentiality measures.

As for the domestic legislation, unfortunately, today in Ukraine there is no law that would regulate the collection and processing of patients' medical data. The main documents for the legal regulation of this direction are the laws of Ukraine "On Information", 1992, "On Protection of Personal Data", 2010, "On Protection of Population from Infectious Diseases", 2000, "On Amending the Law of Ukraine "On Protection of Population from Infectious Diseases", 2020, "On State Financial Guarantees of Medical Services to Population", 2017. However, an analysis of the provisions of the Law of Ukraine "On Information" (Rules of interaction of CPS and patient access, 2020) shows that only the information that is recorded only on a physical medium or displayed in electronic form is protected.

This, of course, does not provide real protection for human rights in information relations. After all, most information about a patient is obtained directly from the patient by the medical worker and is not recorded in documents. At the same time, it is necessary for treatment and should be protected as confidential. In our opinion, this position of the legislator is quite ambiguous, so we consider it advisable to supplement Part. Part 3 of Article 1 of Section I of the Law of Ukraine "On Information" to read as follows: "information is any information and/or data that are stored both on physical media, displayed in electronic form and in unrecorded form".

The 1994 Law of Ukraine "On Protection of Information in Information and Telecommunication Systems" and a number of regulatory documents on technical protection of information (LA TPI) are hopelessly outdated. "Moreover, they oblige public authorities, objects of critical infrastructure facilities and private companies that want to provide services to public authorities, to implement the so-called Complex system of protection of information (CSPI) This, besides being morally obsolete, has proven its ineffectiveness for many years" (Healthcare system, 2020).

It should be noted that in September 2017, the Electronic Health System "E-Health" was developed and implemented, an information and telecommunication system that provides a single information space and data exchange through a central database (Final Rule of the ONC Treatment Law, 2020). The system integrates filing of electronic declarations with family physicians, prescriptions, medical referrals, statistics on coronavirus patients, etc. However, this system, in violation of technical information security requirements, does not actually have a CSP compliance certificate. Therefore, the storage of patient data cannot be called secure. Currently, the Ministry of Health together with the Ministry of Digital Transformation is working on further integration of the E-Health system into the portal and application called "Diia". In order to improve the information security effectiveness of this system, we propose to ensure compliance with HIPAA requirements as a proven and established standard in software development.

It is worth noting the Order of functioning of the electronic health system of Ukraine from 24.05.2018 № 411 (Law of Ukraine, 1992), which for the first time provided for the provisions and control of the maximum information on the collection, processing, storage of information about patients, which is fully consistent with GDPR regulations.

However, this is not enough. It is because of legislative gaps that the protection of this group of data remains unprotected in Ukraine. It is important that in November 2019 an interdepartmental working group was created under the Secretariat of the Ukrainian Parliament Commissioner for Human Rights to develop legislative proposals for the protection of personal data. In addition, a coordination working group was created to develop a bill to amend the Law of Ukraine "On Personal Data Protection" in accordance with the provisions of the GDPR. Although there are currently no significant changes in the domestic legislation. Submitted by the interdepartmental working group under the Ukrainian Parliament Commissioner for Human Rights draft law of Ukraine "On Amendments to the Law of Ukraine", and "On Protection of Personal Data" (on the forms and conditions of consent to the processing of personal data)" from 10.02.2020 № 2671-1, 04.03.2020 returned for revision.

As a consequence, there are numerous cases of security breaches of medical information. For example, the National Cybersecurity Coordination Center (NCCC) under the Security and Defense Council of Ukraine detected a leak of personal medical data from one of the largest clinics in Dnipro during its monitoring. "Among the information that appeared in the public domain were the personal data of the employees and clients of this clinic, in particular, the last name, first name and patronymic, dates of birth, residence addresses, telephone number, e-mail, medical records (which is considered medical information), including results of medical tests, diagnosis, information about the disease, PCR test results, COVID-19 patient lists" (Andriychuk, Strilkina, 2018). The leak occurred as a result of configuration errors in the information systems and databases of clinics that had access to the Internet. It is worth noting that open access to databases gave the opportunity not only to steal personal information, but also to illegally make adjustments to it, including changing prescriptions for drugs, results of medical tests and examinations, and editing records in protocols. The Dnipro Clinic reacted to this fact rather passively, and patient data remained publicly available for quite a long time (Andreychuk, Strilkina, 2018). This fact is a violation of Paragraphs. 13 Item 2 of the General part of the Procedure of functioning of electronic health systems of Ukraine, because the Dnipro Clinic is the administrator of the register, and, accordingly, is responsible for the use of appropriate measures to protect the processed data.

5. Conclusions

Thus, state social policy is a multilevel and functional system that ensures the socio-economic development of the country. It is aimed at ensuring the guaranteed constitutional rights and freedoms of citizens, achieving balance and stability in society,

reducing social tensions and improving their well-being. A qualitative medical reform is possible only with the introduction of modern methods of informatization and, consequently, data protection. As the analysis showed, the legal system of information protection in the medical sphere needs immediate improvement in Ukraine. For this purpose it is necessary: to systematize and codify national legislation in accordance with European legal norms and international law; to develop a comprehensive piece of legislation regulating the collection, protection, and transition of medical information, following the example of GDPR, at the legislative level (structure the medical information system, provide for mandatory certification for information protection, to develop cryptography/encryption technologies, delimit the rights of access to information by medical workers, provide access to information with the mandatory use of electronic signatures, medical workers need to take short courses and register with information security specialists (defined access rights and the ability to change access levels, provide input for identification and authentication), data correction and new information entry is performed with the confirmation of electronic signature, to develop an algorithm of information transition between healthcare facilities); amend the Law of Ukraine "On Protection of Personal Data" (as for the forms and conditions of consent to the processing of personal data); supplement P. 3 of Art. 1 Sec. I of the Law of Ukraine "On Information"; to develop medical information system software in compliance with the GDPR requirements; legislatively enhance the responsibility for violating protection of information in the medical field.

Ukraine, striving to integrate into the European space and building its own strategy of economic development, must be clearly aware of both its capabilities and external influences. Choosing possible alternatives is too difficult a task, but the leading idea of socio-economic policy should remain the desire to ensure sustainable economic development of the country.

References:

Analysis of blokchain technology recommendations to be applied to medical record data storage applications (2020). Available at: https://mecs-press.org/

Andriychuk, A. S., & Strilkina A. A. (2018). Breakdown of the model of keruvannya with access to private medical information. *Radioelectronic and computer systems,* 2(86), 26–32.

Achieving confidentiality in electronic health records using cloud systems (2020). Available at: https://mecs-press.org/

Akhlamov, A. G., & Kusik, N. L. (2011). Economics and financing of health care: teaching method. way, 134 p.

Curogram: a web-based sms app for medical practices (2019). Available at: www.curogram.com

COVID-19 has distributed 3.5 million personal data (2020). Available at: https://www.comnews.ru/content/208448/2020-08-05/2020-w32/covid-19

Kochetkov, A. A. (2005). Fundamentals of economic theory: a course of lectures, p. 472.

FTC Gives final approval to settlement with emergency travel services provider related to allegations it failed to secure sensitive data (2021). Available at: https://www.ftc.gov/news-events/press-releases/2021/02/ftc-gives-final-approval

Healthcare System Technology using Smart Phones and Web Apps (Case Study Iraqi Environment). Available at: https://mecs-press.org/

Fact sheet on interoperability and patient access (2020). Available at: https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

Constitution of Ukraine. Art. 43 (1996).

Martsenyuk, O. G. (2018). The rights of physical and legal entities to medical confidentiality information. Medical Law of Ukraine: Legal Status of Patients of Ukraine and Legislation of Security: Materials of the II All-Ukrainian Conference, 17-18 April, Lviv, pp. 166–171.

Obervan, O. R. (2012). The essence of social policy in the formation of innovative economy in Ukraine. *Efficient economy*, no. 5. Available at: http://www.economy.nayka.com.ua/?op=1&z=1143

Secure multiparty computation for privacy preserving range queries on medical records for star exchange topology (2020). Available at: https://mecs-press.org/

The first penalty for failure to comply with the order of the administrative decision (2018). Available at: https://uodo.gov.pl/pl/138/1889

Rule of interaction between CMS and patient access (2020). Available at: https://iapp.org/news/a/health-care-interoperability-preparing-to-meet-new-privacy-and-security-obligations

Law of Ukraine: About information (1992), 2657-XII. Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text

Tereshko, H. Ya. (2019). Information of civil legal persons in the sphere of medical service. *Medical right*, 1(23), 65–73.

Brazil has access to 16,000,000 patients from COVID-19 (2020). Available at: https://xakep.ru/2020/11/27/covid-leak

U.S. Department of Health & Human services, HIPAA privacy rules for the protection of Health and Mental health information (2020). Available at: https://www.omh.ny.gov/omhweb/russian/hipaa/phi_pro tection.pdf

Healthcare data breaches will cost the industry $ 4 billion (2020). Available at: https://blackbookmarketresearch.newswire.com/news/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-21027640.

General regulation for the acquisition of personal tributes from the European Union (GDPR) (2018), 1725. Available at: http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad

Law on mobility and development of medical insurance (1996). Available at: https://everlegal.ua/hipaa-yak-zakhyschayut-medychni-dani-patsientiv-v-ssha

Final Rule of the ONC Treatment Law (2020). Available at: https://www.healthit.gov/curesrule