ORIGINAL ARTICLE

MEDICAL CONFIDENTIALITY DISCLOSURE IN CONDITIONS OF EPIDEMIC THREATS

DOI: 10.36740/WLek202111203

Tetiana O. Mykhailichenko[1], Oksana P. Horpyniuk[2], Victor Yu. Rak[3]
[1]POLTAVA LAW INSTITUTE OF YAROSLAV MUDRYI NATIONAL LAW UNIVERSITY, POLTAVA, UKRAINE
[2]LVIV STATE UNIVERSITY OF INTERNAL AFFAIRS, LVIV, UKRAINE
[3]M.V. SKLIFOSOVSKY POLTAVA REGION CLINICAL HOSPITAL, POLTAVA, UKRAINE

ABSTRACT

The aim: To establish public opinion on the limits of medical confidentiality in an epidemic and the widespread use of applications that contain personal data, including those regarding health, to understand the possibility of changing the paradigm of public policy to protect medical confidentiality in an exacerbation of the epidemic situation.
Materials and methods: This research is based on regulatory acts, scientific articles, and opinions of both medical workers and ordinary citizens of Poland, Germany, and Ukraine, judicial practice, doctrinal ideas, and views on this issue. Such methods as dialectical, comparative, analytic, synthetic, comprehensive, statistical, and generalization.
Results: the results of a survey of residents of Poland, Germany, and Ukraine showed that one of the pandemic consequences was that a significant number of respondents were willing to partially renounce the right to medical confidentiality in the face of exacerbating epidemic threats to reduce the number of infected.
Conclusions: In the face of the SARS-Cov-2 virus, nations worldwide have faced the challenge of respecting the right to privacy, particularly in terms of medical confidentiality. Virtual methods of patient communication with healthcare professionals use mobile electronic services (applications), and other new technologies in the context of the COVID-19 pandemic have exacerbated the issue of understanding the boundaries of medical confidentiality and personal data protection. In order to maintain an effective balance between human rights and public health, the mass collection and storage of sensitive personal data must take place following the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. At the same time, it is expedient to recommend states to specify specific provisions of this Regulation in order to avoid an expanded interpretation of certain of its provisions.

KEY WORDS: public health, epidemic safe, medical confidentiality, personal data

Wiad Lek. 2021;74(11 p.2):2877-2883

INTRODUCTION

The concept of medical confidentiality has long been known to society[1]. Today, the postulate of prohibiting the disclosure of medical confidentiality is enshrined by the vast majority of countries and is part of the legal guarantees for the protection of human rights and freedoms. At the same time, the COVID-19 pandemic has exacerbated the eternal conflict facing people: individual vs. public interests? Furthermore, the question was raised: what are the limits of protecting confidential information about a person's illness in an epidemic/pandemic and the retention period of such information? A separate challenge was the rapid spread and use of various applications that contain personal data. So, it seems that today society is probably at the next stage of rethinking the boundaries of medical confidentiality

THE AIM

The purpose of this article is to establish public opinion on the limits of medical confidentiality in the face of epidemic threats exacerbation[2] and rapid spread of the use of various applications that contain personal data, including the state of individual's health. This may be the basis for the possibility of changing the paradigm of state policy on the protection of medical confidentiality in an exacerbation of the epidemic situation

MATERIALS AND METHODS

This research is based on regulatory acts, scientific articles, and opinions of both medical workers and ordinary citizens of the Republic of Poland (hereinafter, RP), the Federal Republic of Germany (hereinafter, FRG), and Ukraine. Additionally, judicial practice, doctrinal ideas, and views on this issue have been used. In order to achieve the goals were used a set of general and special scientific approaches as well as the series methods, namely: dialectical, comparative, analytic, synthetic, comprehensive, statistical, and generalization.

RESULTS AND DISCUSSION

The COVID-19 pandemic continues to actively change the face of the world, while more and more variants of this virus (SARS-CoV-2 Alpha, Beta, Gamma, Delta, Lambda) are

constantly appearing [3]. In such a challenging environment, society faces a number of questions: 1) how to strike a balance between respecting the right to medical confidentiality in a pandemic and protecting public health, 2) what is prevalent in an epidemic/pandemic state: individual or public interests, 3) Is it appropriate in an epidemic/pandemic state not to disclose the fact of a particular person infection, 4) what are the limits of protection of medical information about a person's health, 5) what are the current threats of illegal use of personal data stored in various electronic databases? However, this list is not exhaustive, and addressing these issues requires lengthy discussions and in-depth research. Therefore, in our study, we limited the questions range to only three positions.

1. **Medical confidentiality: the concept and liability for its disclosure.** Medical confidentiality is a consequence of the development of civilization, and therefore its concepts and boundaries are closely linked to the level of development of society and its institutions. As it was successfully noted by Rieder Ph., Louis-Courvoisier M., Huber Ph. "Medical confidentiality was and is today a medical and societal norm that is shaped collectively. Any change in its definition and enforcement was and should be the result of negotiations with all social actors concerned" [4]. On the one hand, medical confidentiality is a burden for medical personnel and, on the other hand, a guarantee of their work safety and the quality of its performance. Medical confidentiality is still and will be a matter of the health care system and an ethical dilemma. Its concepts, limits, and conditions of the disclosure are always in the focus of scientists [5-10].

At the international level, the doctor's duty to maintain confidentiality was enshrined by the World Medical Association in the Geneva Declaration (1948): "I will respect the secrets which are confided in me, even after the patient has died" [11]. But what is medical confidentiality? No international legal act contains a clear definition of this concept. At the same time, in each state, regulatory legislation contains provisions on medical confidentiality. In general, medical confidentiality meaning is "the principle of keeping secure and secret from others, the information given by or about an individual in the course of a professional relationship, and it is the right of every patient, even after death" [8]. Also, researchers and practitioners have now developed generally accepted recommendations on the limits of medical confidentiality and the rules of its disclosure [12].

However, health professionals and lawyers are constantly faced with dilemmas about the appropriateness of disclosing confidential health information and addressing the issue of liability for such disclosure. Each country has laws governing the collection, receipt, storage, use, dissemination, ensuring, and protection of confidential information, including the healthcare field. First of all, this right is protected by the Basic Laws of the states. For example, in Art. 51 of the RP's Constitution, Art. 32 of the Constitution of Ukraine, Art. 2 of the FRG Constitution. Also, this right is detailed and specified in other regulations. For example, in Ukraine, these are the Laws "On Information", "On Personal Data Protection", the Fundamentals of Health Care Legislation, "On Psychiatric Care", the Civil Code, etc. In RP – The Patient Rights and Patients Ombudsman Act, The Medical Profession Act, The Civil Code Act, and Code of Medical Ethics which is not considered a legal act [9]. In FRG, the right of every individual to respect and respect for private and intimate spheres and to informational self-determination can be derived from the Basic Law in relation to the state vis-à-vis the citizen (Art. 1 I in conjunction with Art. 2 I GG), the (model) Professional Code of the German Medical Association (MBO), the German Civil Code, etc. [10, p. 290-291]. In addition, each of the states has criminal law provisions that prohibit the disclosure of medical confidentiality and determine the limits of punishment of a person who commits such an offense. In particular, in the Penal Code of RP, it is Art. 266, in the Criminal Code (hereinafter, CC) of Ukraine – Art. 132 and Art. 145, in the CC of FRG – Section 203. How often are convictions handed down for these offenses? Quite rarely. Thus, for example, according to the Unified State Register of Judgments of Ukraine, only one sentence was passed under Art. 132 of the Criminal Code of Ukraine (judgment of the Central District Court of Simferopol dated 22.01.2013, case № 122/9610/2012) on the disclosure of medical confidentiality [13].

Some cases have also been considered by the European Court of Human Rights (for example, "Panteleyenko v. Ukraine" (Application no. 11901/02) 29.06.2006, "L.L. v. France" (Application no. 7508/02) 10.10.2006, "Armonas v. Lithuania" (Application no. 36919/02) 25.11.2008, "Biriuk v. Lithuania" (Application no. 23373/03) 25.11.2008, "Avilkina and Others v. Russia" (Application no. 1585/09) 06.06.2013, "L.X. v. Latvia" (Application no. 52019/07) 29.04.2014, "Konovalova v. Russia" (Application no. 37873/04) 09.10.2014, "Sidorova v. Russia" (Application no. 35722/15) 28.05.2019 etc.

The question of the expediency of using the terms "doctors secret" and "medical confidentiality" is also debatable today. Researchers claim that doctors' secret is a more slang term, and the wording of medical confidentiality is more appropriate because not only doctors but also other healthcare professionals and staff are in contact with patients during treatment. Thus, the scope of people who are in touch with the information that they are obliged to keep as a secret of the patient is not limited to the doctor only [14, p. 206]. We could agree with this caveat because "doctors secret" is a subjectively narrower concept. Instead, "medical confidentiality" fully reflects the reality, encompassing not only doctors but also junior medical staff and persons who have become aware of confidential information in connection with the performance of professional or official duties.

In order to protect the rights of patients and medical professionals (also including from state's interference), the legislation prescribes cases when the disclosure of medical confidentiality is lawful. Usually, a person can disclose confidential information if 1) the individual has given consent, 2) the information is in the public interest (that is, the public is at risk of harm due to a patient's condition),

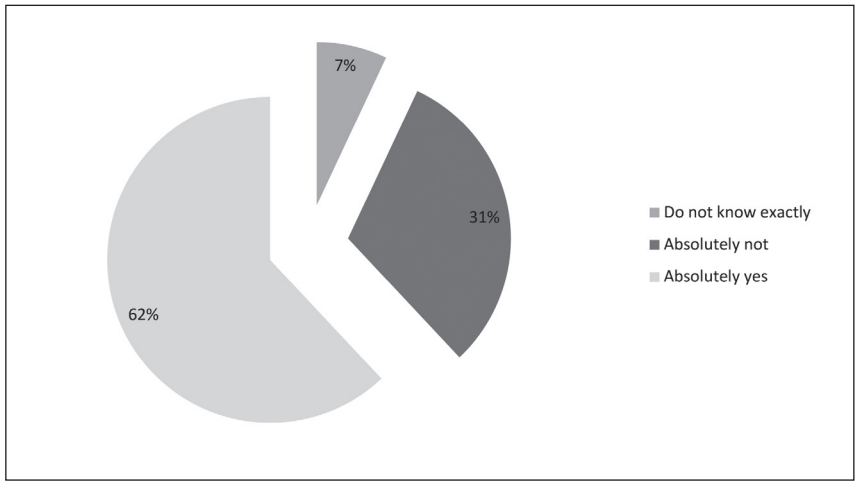

Fig. 1. The answer of the respondents of the second group regarding the disclosure that the person is ill, in the epidemic conditions

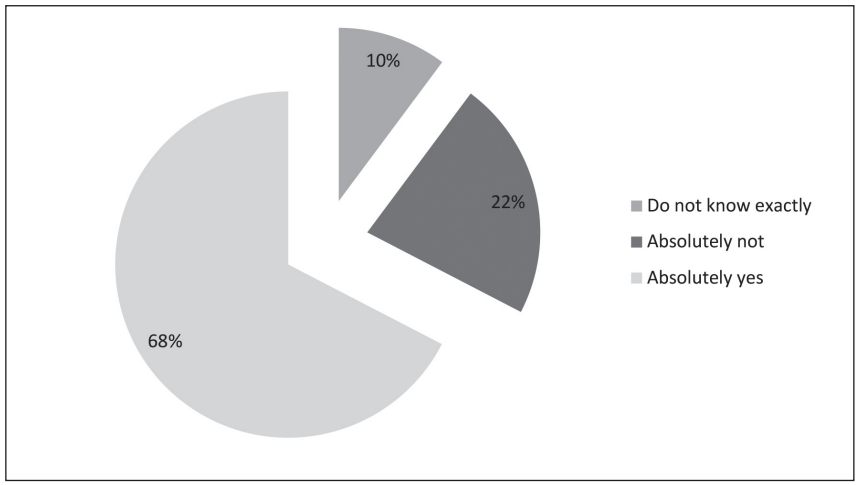

Fig. 2. The answer of the respondents of the first group regarding the disclosure that the person is ill, in the epidemic conditions

3) disclosure is compelled by law (often public risk issues are covered by laws that compel disclosure, such as for positive test results for HIV/AIDS) and 4) the information is in the public domain already [15]. Exactly the second exception is of interest in our study. As the authors of the publication emphasize, "You may disclose information to prevent 'serious or imminent threat to the life or health of the individual concerned, or another. An example is if you become aware of information that could result in a disease epidemic" [15]. So, the logical question arises: is it advisable for a healthcare professional to keep a secret of the fact of person's infection in an epidemic/pandemic?

2. **The expediency of medical confidentiality in the face of epidemic threats.** Today, there seems to be a need to review or confirm the current limits of medical confidentiality. We may not focus on the time of Hippocrates when only one doctor examined the patient. Today, in addition to health workers, access to medical information is available to a number of others through the introduction of health insurance, active digitalization of society (electronic data storage systems, mobile applications) [16], and most importantly – modern society is faced with the rapid and hard-to-control spread of coronavirus infection. SARS-CoV-2 and its strains.

As already noted, the concept of medical confidentiality and its boundaries are changing along with the development of our society [3]. In such circumstances, it seems appropriate to raise the question: will the COVID-19 pandemic become the driving force that will once again change the boundaries of medical confidentiality. We surveyed residents of Ukraine, Poland, and Germany: medical workers (Group I, 100 people) and ordinary citizens (Group II, 300 people) on a number of issues. And this poll seems to have shown that a pandemic could be another starting point for a new paradigm.

Thus, answering the question "Do you consider it permissible to disclose data that a person is sick in an epidemic" only 31% of respondents in group II replied, "categorically no". Another 7% did not have an exact answer to this question. Furthermore, as many as 62% agreed because it can help reduce the infection spread. It is noteworthy that from this group, 49.7% of people had coronavirus infection, 28.3% – not, 21.4% – do not know exactly, and 0.6% did not want to answer this question. At the same time, when surveying health professionals regarding the question "Do you consider it permissible to disclose data that a person is sick in an epidemic" 22.4% answered "absolutely not", 10.2% – do not know the answer to this question and 67, 4% of respondents consider it appropriate. That is, in general, 61.7% of respondents understand the need to change the view on the limits of strict protection of medical confidentiality in the face of epidemic threats, which is clearly seen in the diagrams below. (Fig. 1 and 2).

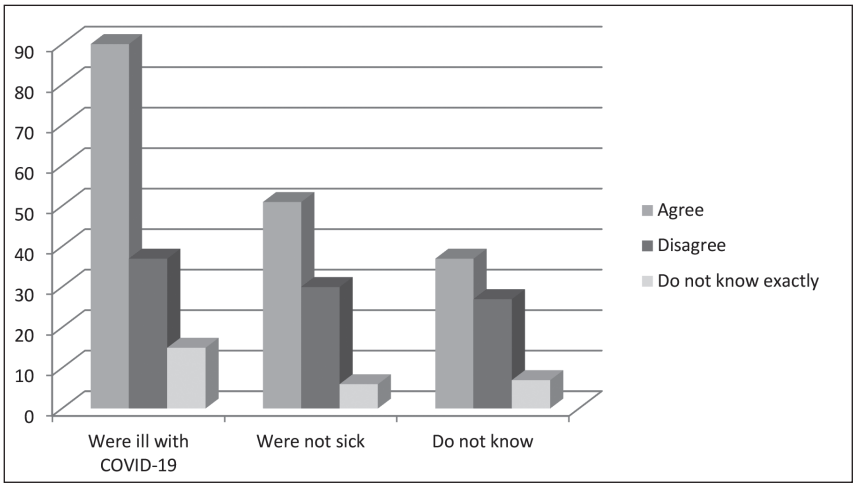

Fig. 3. Correlation between the presence of the disease and the attitude towards disclosure

Respondents from regional centers, district centers, and rural areas were involved in the survey of both medical professionals and ordinary citizens. And 66.7% (64 people) of surveyed health professionals live in regional centers. From their total number answering the question: "Do you consider it permissible to disclose data that a person is ill in an epidemic?" 72% of respondents answered affirmative, 20% of respondents were categorically against the disclosure, and the rest chose "I do not know". Representatives of medical professionals from district centers and rural areas were 33.3% (36 people). Of these, 67% of respondents believe that information about sick people should be available in an epidemic, 5.5% voted against such an approach, and 27.5% had no answer.

75.3% of Group II respondents (230 people) live in regional centers. Of their total number, 56.5% are convinced that disclosing medical secrets in the face of epidemic threats will help reduce the number of infected people, 33% believe that this is unacceptable, and 10.5% chose the option "I do not know". The number of respondents from district centers and rural areas is 24.7%. At the same time, out of 70 people, 83% voted for the dissemination of information, 11% (8 people) – categorically against disclosure, and 6% did not decide on the answer.

In general, we see that the vast majority of respondents from rural areas, district centers, and regional centers believe that the disclosure of medical confidentiality in the face of epidemic threats is justified, while residents of rural areas and small towns are more inclined to the necessity of disclose.

In our opinion, such results can be explained by: 1) a smaller population in district centers and rural areas, which results in 2) closer ties between the inhabitants of these settlements and 3) faster dissemination of information.

In general, this thesis is confirmed by the following information: most often, the expediency of disclosure is emphasized by those respondents of group II who became ill with COVID-19 (63.38%), while the lowest percentage of those who are committed to "concessions regarding the right to medical confidentiality" does not know whether they were sick (52.11%). At the same time, regardless of the category of respondents, the majority still agree with the expediency of disclosure in order to reduce the infection spread rate. Correlation between the presence of the disease and the attitude towards disclosure is presented in Figure 3.

It is clear that in order to adjust the current regulative provisions, one should first conduct a large-scale opinion poll and evaluate all the pros and cons of such changes. However, on the other hand, the results of our survey seem indicative and may form the basis of further, more in-depth research.

3. **Use of applications to control the epidemiological situation and the issue of relevant personal data storing.** As a result of the coronavirus pandemic, states have begun using a variety of programs to communicate with medical staff and patients, monitor their health, and people's compliance with self-isolation through the use of mobile services and cell phone surveillance software. Appropriate software has been developed to monitor the symptoms of COVID-19, map the population movements, monitor contacts of infected persons, execute quarantine orders, etc. In turn, this has caused the need to ensure the confidentiality of medical data and proper cybersecurity of relevant software and mobile services (applications), which is now actively discussed in society [17-18; 19, pp. 27-31]. Australia, China, Israel, Norway, Singapore, and South Korea were among the first to introduce mobile-based contact tracking. In the United States, there is a need to remove restrictions on access to communication programs for specific categories of people, so it was allowed to use Apple FaceTime, Facebook Messenger, Google Hangouts, Zoom and Skype, etc., for communication. [17]. RP launched the Kwarantanna Domowa mobile service. In Ukraine, for citizens crossing the state border, a mobile application of the electronic service "Act at home" was also introduced [22].

At the same time, it should be noted that the degree of interference with a person's privacy or the level of tracking of persons in need of self-isolation through mobile services varies among the countries. Due to the general privacy policy in the countries of the Asian region, stricter

control over the population has been established there. For example, in Singapore, the Trace Together application was created, which not only monitors a person's compliance with the self-isolation mode but also records the phones of people with whom the person who installed the application is in contact via Bluetooth. In China, the authorities did not develop any applications but instead tracked the movement of citizens via GPS coordinates or the use of bank accounts [23].

It should be emphasized that many human rights defenders, specialists in the field of law (N. Korshivsky [24], C. Veliz [18, p. 110], M. French, A. Guta, M. Gagnon, and others [25]) challenge the effectiveness of such applications to reduce the level of infection spread [18, p. 112]. Regarding the respondents of the first group, when asked about the effectiveness of using the mobile application of the electronic service to reduce the epidemic tension on a five-point scale, the majority (36%) focused on mark three. At the same time, among the surveyed respondents of group II, the majority (46.5%) indicated zero efficiencies of the mobile application. Such a response rather indicates a low awareness of the population about the primary purpose of implementation and the use of this electronic service or distrust of the government. In addition, this answer to the question about the effectiveness of the application is associated with a low percentage of use of this service because 76% of the respondents of group II indicated that they did not try the application.

Today, the threat to privacy from the uncontrolled use of personal data, including sensitive (vulnerable) personal data, should be noted through applications. It seems that they can be divided into three main types:

1. Threats of various kinds of abuse by the authorities and/or large private corporations. In the long run, the confidential data obtained during the pandemic period can be illegally used by both governmental and non-governmental organizations for marketing purposes to influence the behavior of active users of social networks, and so on[3]. In addition, large technology companies now gain more power than government institutions.
2. Threats related to cybercrime: today, electronic systems of health care facilities that store personal medical information about patients and biometric data are under threat more than ever before. Although many people believe that biometric authentication systems cannot be hacked or tricked, biometrics is not as reliable as they think[4].
3. Threats related to discrimination, undermining the reputation of certain ethnic groups or national minorities[5]. After all, information about health and habits can be especially vulnerable in the case of employment and insurance [19, pp. 27-31]. Detection of disease through digital technology in certain religious or ethnic groups can also lead to various forms of harassment and violence.

However, despite the existing threats to privacy, under certain conditions, namely the controlled use of mobile services, mobile phone tracking programs to identify risks of COVID-2019 infection and prevent this disease, the pandemic can be stopped, and they could be of help to physicians who fight the disease. After all, most of the respondents we interviewed, as noted, allow the disclosure of data on the disease of a person in an epidemic because it can help reduce the spread of infections. However, in order for users of mobile services to help stop the spread of diseases, states must ensure these programs to be user-friendly, the legality, clarity, and accessibility of the rules of processing and storage of personal data, their reliable protection.

The use of such mobile services must be strictly regulated. In particular, Regulation of the European Parliament and of the Council 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 defines clear principles of personal data processing in automated systems, databases (Article 5): 'lawfulness, fairness and transparency'[6], 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation'[7], 'integrity and confidentiality' and 'accountability' [27]. At that time, the poll showed that state officials often violate its requirements, which, in our opinion, may further exacerbate the conflict between individuals and government institutions.

---

[1] Traditionally, the cure for the medical secrecy concept development begins with the appearance of the Hippocratic oath. However, some researchers note that this concept earlier appeared in ancient India, where the rule was: "You can be afraid of a brother, mother, friend, but never – a doctor!" [1].

[2] Hereinafter we will talk about epidemic threats coming from viruses that are characterized by high virulence and contagiousness.

[3] For example, one of the most high-profile privacy scandals is related to Cambridge Analityca, when the company used the personal data of more than 87 million users to build psychological profiles of voters around the world to develop personalized political propaganda and election influence [18, pp. 108].

[4] For example, in 2011 Israeli authorities announced that the entire national biometric database they owned had been stolen, along with information on names, dates of birth, social security card numbers, family members, immigration dates, and medical records. of the Israelites. This information was stolen by a contractor and sold to a criminal corporation, which later made it fully available online in the digital underground. That provided additional opportunities for a wide range of crimes [26, p. 397].

[5] In South Korea, for example, cell phone tracking has been used to confirm the link between infections and a number of LGBT nightclubs, which has provoked a backlash against a marginalized group. And in Guangzhou, China, dozens of Africans have reported evictions and other discriminatory treatment due to misrepresentation of connection with COVID-19 [25].

[6] The Norwegian National Data Protection Authority (Datatilsynet), which allowed data processing without depersonalization to track the smartphones of COVID-2019 contacts in case of impossibility to draw accurate conclusions, raised some reservations about maintaining a balance between privacy and protection of public health interests. [20]. It should be noted that among the respondents of the II group surveyed by us (ordinary citizens) 73.3% indicated that they were not informed about the purpose of collecting their personal data during COVID-19 and 66.7% did not consent to the processing of these data.

[7] The survey of respondents of group II showed that 89.2% did not aware of the subsequent use of personal information provided by persons during self-isolation through a mobile application. In addition, 81.1% of respondents indicated that they were not informed about the period of storage and deletion of the information provided. As for the retention period of the collected personal data, 39.8% believe that they should be deleted immediately after the end of self-isolation or recovery of the person; 22% – 14 days after the end of self-isolation or recovery; 19.5% – after the end of the active phase of the disease; another 18.7% – 30 days after the end of quarantine.

CONCLUSION

Thus, it can be stated that virtual means of communication between patients and healthcare professionals, the use of mobile electronic services (applications), and other latest technologies in conditions of increased risk of infection have exacerbated the understanding of medical confidentiality and protection of personal data collected during the COVID-19 pandemic. The survey shows that a significant number of respondents recognize the expediency of disclosing the fact of infection of a person in the face of increased epidemic threats. However, mass collection of personal sensitive data and non-compliance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data further may lead to exacerbation of social conflict. Therefore, we consider it appropriate to recommend that national governments to specify certain provisions of this Regulation (for example, on the amount of personal data collected, the retention period of such information, the procedure and timing of its destruction) in order to avoid broad interpretation of certain its provisions and to ensure a balance between private and public interests. Although previous polls show that society, in general, is ready to change the paradigm of public policy to protect medical confidentiality in the face of an epidemic situation escalation.

REFERENCES

1. Argunova YU. N. Prava grazhdan pri okazanii psikhiatricheskoj pomoshchi [The rights of citizens in the provision of psychiatric care]. Moskva: Grifon, 2014. 640 c. (Ru).
2. Tracking SARS-CoV-2 variants. WHO. Available from https://www.who.int/en/activities/tracking-SARS-CoV-2-variants/
3. Rieder Ph., Louis-Courvoisier M., Huber Ph. The end of medical confidentiality? Patients, physicians and the state in history. Med Humanit. 2016 Sep; 42(3): 149–154. doi: 10.1136/medhum-2015-010773
4. Ablamskyi S. Ye., Romaniuk V. V., Chycha R. P., Ablamska V. V. Temporary access to documents containing medical confidentiality (criminal procedural aspect). Wiad. Lek. 2020;73(5):1032-1036. doi: 10.36740/WLek202005136.
5. Horodovenko V. V., Pashkov V. M., Udovyka1 L. G. International legal instruments in the field of bioethics and their impact on protection of human rights. Wiad. Lek. 2020;73(9 p. II):2056-2061. doi: 10.36740/WLek202007144.
6. Klepka D. I., Krytska I. O., Sydorenko A. S. Obligation of the disclosure of medical confidential information in criminal proceedings. Wiad. Lek. 2019;72(12 p. II):2602-2608. doi: 10.36740/WLek201912235
7. Plebanek E. Ujawnienie tajemnicy lekarskiej w procesie karnym a odpowiedzialność karna lekarza. Białostockie Studia Prawnicze. 2020;25(2):65-98. doi: 10.15290/bsp.2020.25.02.04
8. Bourke Ju., Wessely S. Confidentiality. BMJ. 2008;336(7649):888–891. doi: 10.1136/bmj.39521.357731.BE
9. Jaroszyński Ja., Husarz R., Jurek A., Mela A. Doctor-patient confidentiality – right and duty of a doctor in law regulations. Journal of Education, Health and Sport. 2018;8(3):444-452. doi: http://dx.doi.org/10.5281/zenodo.1207230
10. Parzeller M., Wenk M., Rothschild M. Zertifizierte Medizinische Fortbildung: Die ärztliche Schweigepflicht. Dtsch Arztebl. 2005;102(5):A 289-296.
11. WMA Declaration of Geneva. Adopted by the 2nd General Assembly of the World Medical Association, Geneva, Switzerland. September 1948. Available from: https://www.wma.net/policies-post/wma-declaration-of-geneva/
12. Confidentiality: protecting and providing information. General Medical Council. April 2004. Available from: https://www.gmc-uk.org/-/media/documents/confidentiality-2004---2009-55664503.pdf?la=en
13. Yedynyi derzhavnyi reiestr sudovykh rishen [Unified state register of court decisions] Available from: http://reyestr.court.gov.ua/
14. Dragana D. Medical Secret as a Basis of Medical Confidence in Relation Doctor-Patient – a View from Healthcare System of the Republic of Serbia Jahr : Europski časopis za bioetiku. 2018;9(2):205-222.
15. Understanding medical confidentiality and privacy laws for health professionals. https://www.slatergordon.com.au/blog/featured/understanding-medical-confidentiality-and-privacy-laws-for-health-professional
16. Unachukwu A. Medical Confidentiality: What Does it Mean to the Vulnerable? https://www.academia.edu/29756371/Medical_Confidentiality_What_Does_it_Mean_to_the_Vulnerable
17. Jalali M. S., Landman A., Gordon W. J. Telemedicine, privacy, and information security in the age of COVID-19. Journal of the American Medical Informatics Association. 2020;28(7):1-2. doi:10.1093/jamia/ocaa310
18. Veliz C. Privacy During Pandemic and Beyond. The Philosophers Magazine. January 2020. p. 107-113. doi:10.5840/tpm20209075
19. Boudreaux B., Denardo M. A., Denton S. W. et al. Data Privacy During Pandemics: a Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance Programs. RAND Corporation, Santa Monica, Calif. January 2020. 143 p. doi:10.7249/RRA365-1
20. Magklaras G., Lo'pez-Bojo'rquez L. N. A review of information security aspects of the emerging COVID-19 contact tracing mobile phone applications. Norwegian Center for Molecular Medicine, University of Oslo, Norway and Steelcyber Scientific. May 2020. doi:10.13140/RG.2.2.34790.65606
21. Aplikacja Kwarantanna domowa. Koronawirus: informacje i zalecenia. Available from: https://www.gov.pl/web/koronawirus/kwarantanna-domowa
22. Instruktsiia z vykorystannia elektronnoho servisu «Dii vdoma» Yedynoho derzhavnoho veb-portalu elektronnykh posluh dlia vyrishennia pytannia shchodo observatsii (izoliatsii) osib, yaki peretynaiut derzhavnyi kordon abo vizhdzhaiut z tymchasovo okupovanykh terytorii u Donetskii ta Luhanskii oblastiakh, Avtonomnoi Respubliky KRYM i Sevastopolia [Instructions for using the electronic service "Act at home" of the Unified state web portal of electronic services to address the issue of observation (isolation) of persons crossing the state border or entering from the temporarily occupied territories in Donetsk and Luhansk regions, the Autonomous Republic of Crimea and Sevastopol]. Available from: https://www.kmu.gov.ua/storage/app/sites/1/18%20-%20Department/18%20-%20PDF/04.2020/instrukciya-diy-vdoma.pdf (in Ukrainian).
23. Shcho ne tak z dodatkom Dii «Vdoma»? [What's wrong with the app Action 'AtHome'?] LB.ua. Available from: https://lb.ua/society/2021/04/26/483087_shcho_z_dodatkom_dii_vdoma.html
24. Korshivskij N. Global'nyj vyzov vs privatnost': personal'nye dannye v usloviyakh pandemii [Global challenge vs privacy: personal data in a pandemic]. Liga.Tech. Available from: https://tech.liga.net/technology/opinion/globalnyy-vyzov-vs-privatnost-personalnye-dannye-v-usloviyah-pandemii (in Russian).
25. French M., Guta A., Gagnon M. et al. Corporate contact tracing as a pandemic response. Critical Public Health. Published: October, 2020. doi: 10.1080/09581596.2020.1829549

26. Hudmen M. Zlochyny maibutnoho [Crimes of the Future] / Per. z anhl. I. Mazarchuk, Ya. Mashyko. Kharkiv: Vyd-vo «Ranok»: Fabula, 2019. 592 p. (in Ukrainian).
27. Regulation (EU) 2016/679 of the European Parliament and of the Council 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/EU. 27 April 2016. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

ORCID and contributionship:
Tetiana O. Mykhailichenko: 0000-0002-4668-3375 [C,D,E,F]
Oksana P. Horpyniuk: 0000-0003-3110-6564 [B,D,E,F]
V. Yu. Rak: 0000-0003-4427-9907 [A,D,E,F]

Conflict of interest:
The Authors declare no conflict of interest

CORRESPONDING AUTHOR
Tetiana O. Mykhailichenko
Poltava Law Institute of Yaroslav Mudryi National Law University
Poltava, Ukraine
tel: +380976437653
e-mail: myhailichenko_t@yahoo.com

Received: 17.06.2021
Accepted: 14.10.2021

A – Work concept and design, **B** – Data collection and analysis, **C** – Responsibility for statistical analysis, **D** – Writing the article, **E** – Critical review, **F** – Final approval of the article