REVIEW ARTICLE

CONTENTS

Challenges of ensuring the protection of personal and other medical data in the field of transplantation and reproductive technologies in the digital environment

Zaborovskyy Viktor, Manzyuk Vasyl, Fennych Vasyl, Shchoka Stanislav
UZHHOROD NATIONAL UNIVERSITY, UZHHOROD, UKRAINE

ABSTRACT

Aim: To study the legal, technical, and organisational issues of ensuring the confidentiality of personal and other medical data, in particular, in the context of the use of mobile medical applications (mHealth), various sets (bases) of medical data, in transplantology and the use of ART.

Materials and Methods: The research materials comprised scholarly publications, legal acts, analytical reports from international organizations, and judicial practice relating to the problems of ensuring confidentiality and protection of personal and medical data in healthcare, particularly in transplantology and ART within the digital environment. The search for sources was conducted using international and national scientometric and legal databases, including PubMed, Scopus, and Web of Science, as well as official repositories of regulatory and legal acts of the European Union, the United States, and Ukraine. The chronological scope of the search covered the period from 2015 to 2025, which is justified by the rapid development of digital medicine, mobile health applications (mHealth), biobanks, and the growing incidence of cyber threats in the healthcare sector during this time frame. The search was conducted using the following keywords and their combinations in Ukrainian and English: confidentiality of medical data, personal data, digital medicine, mHealth, cybersecurity, protection of medical information, transplantology, and ART.

Conclusions: Confidentiality is a fundamental component of the relationship between a doctor and a patient, which should be based on mutual trust, especially in the field of transplantology and the use of ART, which require medical professionals not only to clearly apply the norms of legislation in this area, but also to adhere to high moral and ethical standards of professional activity, taking into account, the need for permanent exchange of information between many participants in such special legal relations.

KEY WORDS: confidentiality, medical data, personal data, digitalization of medicine, mHealth applications, transplantology, ART

Wiad Lek. 2026;79(2):440-447. doi: 10.36740/WLek/218723 DOI

INTRODUCTION

In the context of the rapid development of the use of digital technologies, especially in the field of health care (and particularly in the field of transplantology and reproductive technologies), the issue of ensuring the confidentiality of personal and other medical data is gaining particular importance. The introduction of mHealth applications, biometric and genetic technologies, as well as the expansion of the scope of application of additional reproductive technologies and transplantology, significantly expands the volume and sensitivity of medical information that is processed. This, in turn, leads to the emergence of new challenges related to cybersecurity, data deanonymization, commercial use of personal information without the consent of the subject, as well as the insufficient effectiveness of existing legal control mechanisms.

The relevance of this work also lies in the need to study the problem of ensuring trust between participants in medical legal relations, which is the basis for the effective functioning of the health care system, in particular, in the field of transplantology and reproductive technologies. In view of the above, the study of legal, organisational, and technical aspects of protecting medical information is extremely relevant both at the national and international levels.

Among the scientists who have studied individual aspects of this issue, it is appropriate to single out the works of S. Alder, P. Burcher, K. Cato, D. Chirra, D. Chornenka, R. Gupta, N. Hammond-Browning, C. Horner, S. Hosseini, P. Huyvan, R. Iyengar, S. Ikeda, S. Iribarren, H. Luu, M. Mello, A. Musienko, O. Omelchenko, V. Pishta, M. Sharma, A. Schwab, K. Spector-Bagdady, P. Stone, N. Williams and others. At the same time, a comprehensive

study of this issue, as well as the identification of ways to solve it, remained virtually unnoticed by scientists.

AIM

To study the legal, technical, and organisational issues of ensuring the confidentiality of personal and other medical data, in particular, in the context of the use of mobile medical applications (mHealth), various sets (bases) of medical data, in transplantology and the use of ART.

MATERIALS AND METHODS

Various methods of scientific knowledge form the methodological basis of an interdisciplinary approach, which includes a set of methods that allow us to study the social and legal aspects of ensuring the confidentiality of medical information in the context of the digital transfor mation of health care, especially in the field of transplantology and reproductive technologies.

The research materials comprised scholarly publications, legal acts, analytical reports from international organizations, and judicial practice relating to the problems of ensuring confidentiality and protection of personal and medical data in healthcare, particularly in transplantology and ART within the digital environment. The search for sources was conducted using international and national scientometric and legal databases, including PubMed, Scopus, and Web of Science, as well as official repositories of regulatory and legal acts of the European Union, the United States, and Ukraine.

The chronological scope of the search covered the period from 2015 to 2025, which is justified by the rapid development of digital medicine, mobile health applications (mHealth), biobanks, and the growing incidence of cyber threats in the healthcare sector during this time frame. The search was conducted using the following keywords and their combinations in Ukrainian and English: confidentiality of medical data, personal data, digital medicine, mHealth, cybersecurity, protection of medical information, transplantology, and ART. In total, more than 50 sources were analyzed in this study, including peer-reviewed scholarly articles, international guidelines, regulatory instruments (GDPR, HIPAA), court decisions, and analytical reports from specialized medical organizations.

The inclusion criteria for sources comprised: relevance to the protection of medical data in the digital environment, with emphasis on healthcare, particularly transplantology and/or ART; the presence of a clearly articulated legal, ethical, or cybersecurity-related analysis; publication in peer-reviewed academic journals or official sources. The limitations of the study consisted in the exclusion of sources that did not correspond to the research subject or were purely descriptive in nature, as well as those lacking substantiated conclusions or failing to account for the specificity of the digital environment and contemporary cybersecurity challenges.

ETHICS

All sources used in this literature review are publicly available.

REVIEW AND DISCUSSION

MODERN CHALLENGES AND THREATS TO THE CONFIDENTIALITY OF MEDICAL DATA IN THE DIGITAL AGE

The impact of information technology, in particular, on the health care sector, as well as the problems of ensuring the confidentiality of personal and other medical data of an individual, have repeatedly been the subject of our scientific research [1-4]. A significant problem in ensuring the confidentiality of personal and other medical data of an individual lies in their actual separation from other related data about the individual, as well as taking into account the diversity of sources of obtaining such information. Based on the fact that the clinical use of personal genetic and other personal data of an individual is rapidly growing, unprecedented volumes of personal data are generated and distributed in many other contexts, such as mobile application technologies, intelligent personal and home devices, online activity and the use of biometric technologies, a number of scientists question the feasibility of entering a new era of digitalization while abandoning confidentiality when using new technologies [5]. In the work «Consumer Perspectives on Privacy Protection and Sharing of Personal Digital Health Information», scientists have drawn attention to the fact that, on the one hand, interaction with the health care system and the use of mobile devices, social networks, phone applications, and retail create a huge amount of digital data reflecting a person's private health, and on the other hand, the growing collection of digital health information and the blurred boundaries between medical data and data that do not directly relate to a person's health raise concerns about the possibility of ensuring their confidentiality and security, which in some ways even contradict the benefits that such data can provide [6]. A striking example of this is the high-profile case Dobbs v Jackson Women's Health [7], in which the US Supreme Court focused, among other things, on the justified

concern that information from women's applications (for example, for tracking menstrual cycles) and for purchases on websites may contain confidential medical data, in particular, on reproductive health.

The issue of ensuring the confidentiality of personal and other medical data of an individual processed by mobile applications that are in some way related to the field of health care (mHealth applications) has been repeatedly the subject of scientific research. Without questioning the advantages that mHealth applications provide in terms of improving access to health care resources and monitoring the health status of an individual in real time [8], there are quite justified concerns about ensuring the confidentiality of the information they access, its commercial use (sale of subscriptions and sharing of user data), and inadequate compliance with privacy standards in general [9].

Although the EU, the USA and many other countries around the world have developed standards (regulations) for the protection of personal data and other confidential information of individuals, including in the health care sector (for example, in the European Union this is the General Data Protection Regulation (GDPR) [10], in the USA – the US Health Insurance Portability and Accountability Act (HIPAA) [11] and the Post-Market Management of Medical Device Cybersecurity [12]), research in this area indicates the difficulty in implementing these standards in practice and the presence of cases of unauthorized collection and distribution of data obtained from applications, in particular in the health care sector.

A study conducted by the Norwegian Consumer Council found that a number of popular applications, including those in the health and fitness sector, shared data with advertising companies without the user's informed consent [13]. A fundamental study into the privacy disclosures of mHealth applications was carried out by Australian researchers who conducted a large-scale analysis of over 20,000 applications available on Google Play (the largest mobile application marketplace). Their study found that the vast majority of applications (88%) could access and potentially share personal data, but compared to basic non-health applications, mHealth applications included fewer data collection operations in their code, transferred less user data, and demonstrated lower levels of third-party intrusion. At the same time, an analysis of the privacy policies of such applications, namely the actual transfer of user information, raised concerns, as 28.1% of mHealth applications did not offer any privacy policy text, and at least 25% of user data transfers violated what was stated in their privacy policies. Based on this study, Australian researchers conclude that the collection of users' personal information is a common practice in mHealth applications and is not always transparent and secure, and users (patients) are often not properly informed about the privacy practices of these applications and the associated privacy risks before installing and using them. Many applications in the field of medicine, health and fitness are opaque in their work and collect user data (including on behalf of hundreds of third parties) and have the potential to share data with third parties, including advertising and tracking services [14]. Many other researchers, including K. Spector-Bagdady and M.M. Mello, point out that there are many cases not only when Internet providers transfer mobile device user data to law enforcement agencies without sufficient legal grounds, but also cases of selling commercially collected user data to third parties [15].

CYBER THREATS IN DIGITAL MEDICINE: THE PROBLEM OF PERSONAL DATA LEAKAGE

Information technologies not only create new opportunities for people, but also generate new threats. The rapid development of telecommunication and computer technologies contributes to the fact that the exchange and processing of information has become more voluminous and easy, respectively, but the problem of protecting personal data from such violations of the rights of their carrier, as information leaks, unauthorized or accidental access to it, illegal copying, destruction, modification, blocking, and distribution is becoming increasingly relevant [16]. O. Omelchenko rightly notes that today, not only is the physical safety of a person relevant, but also their information security, which is becoming even more vulnerable due to the capabilities of the latest technologies [17]. In recent years, not only has the number of Internet users increased, but the form of their connection has also changed (from personal computers and mobile phones to everyday objects, such as «smart» household appliances, vehicles, and other devices connected to the network), which has complicated the procedures for cybersecurity and protecting the privacy of individuals in the digital age [18]. A.V. Musienko and V.V. Musienko hold an almost similar position, since the deepening of the digital transformation of society (for example, «a country in a smartphone»), in their opinion, along with the advantages, also increases the vulnerability of society to cyber threats, which requires strengthening cybersecurity not only in a particular country, but also in a global dimension, since network systems spread throughout the world [19].

The rapid development of information and innovative technologies, in particular in the field of healthcare,

unfortunately leads to the emergence of new illegal ways of obtaining personal and other medical data of an individual, new manifestations of criminal acts, and therefore to the need for permanent updating of methods of countering them. Leakage of medical data is not a new phenomenon, and over the past ten years, the following statistical data can be cited. Thus, one of the world leaders in the field of cybersecurity, Trend Micro Incorporated, conducted an analysis, as a result of which it was confirmed that in 2015 alone, 113.2 million medical records were stolen, which were used by attackers to illegally purchase medicines, commit tax fraud and other illegal actions [20]. In 2017, a ransomware attack (WannaCry) affected more than 200,000 devices in 150 countries, which led to mass chaos and suspension of medical services in many parts of the world [21]. The media also describes Google's attempt to enter the lucrative US healthcare market, namely through Project Nightingale, to obtain and process personal medical data of up to 50 million non-anonymised customers of Ascension, one of America's largest healthcare providers, without notification or consent from patients or their doctors [22].

While the use of digital technologies during the COVID-19 pandemic has undoubtedly had a significant positive impact on healthcare, education, pensions and other social security, this period has also been characterised by an unprecedented surge in cyberattacks, following the increase in the amount of personal data processed as a result of the pandemic. For example, in 2020 alone, more than 400 organisations and 20 million people in the US healthcare system were affected by cyberattacks [23].

In February 2024, Change Healthcare was attacked by ransomware, which resulted in the encryption of files and the theft of protected health information of approximately 190 million people. This leak was the largest leak of medical data (names, contact information, dates of birth, Social Security numbers, and other medical information) in US history and led to a disruption that lasted several weeks and seriously hampered the work of many healthcare institutions [24].

Overall, ransomware attacks have become one of the most serious and widespread threats to the healthcare sector in recent years. Critical patient data, confidential information, and even potentially catastrophic service disruptions are attractive targets for cybercriminals, as noted by R. Chirra [25].

According to Microsoft Threat Intelligence, healthcare was one of the most affected industries last year, and ransomware attacks have increased by 300% in recent years (one of the factors is Russia providing a safe haven for ransomware groups). In 2024, nearly 400 US healthcare facilities were affected by ransomware, causing network outages, offline systems, delays in critical medical procedures, and rescheduled appointments, costing facilities up to $900,000 per day in downtime alone [26].

PECULIARITIES OF ENSURING CONFIDENTIALITY IN THE FIELD OF TRANSPLANTOLOGY AND APPLICATION OF REPRODUCTIVE TECHNOLOGIES

Despite all the positive aspects of the development of the field of transplantology and additional reproductive technologies, the issue of ensuring the confidentiality of personal and other medical data of all participants in medical-legal relations remains important. This issue has repeatedly been the subject of scientific research, and in many cases, scientists focus their attention on the problem of ensuring a balance between the need to form large databases containing primarily medical data of patients and the need to ensure their confidentiality [2].

Protection of private, in particular, personal and medical data of a person is an element of a comprehensive information protection system that must ensure not only the personal security of a person (protect the inviolability of private life), but also maintain a balance of interests of the individual, society and the state in the field of information processing [27]. Society, the state, and each individual, on the one hand, are interested in increasing the amount of medical information, and on the other hand, it is necessary to create appropriate conditions for their collection, storage and protection, primarily in cyberspace. As V.I. Pishta rightly notes, the Ukrainian legislator must develop special legal norms to regulate relations in the field of healthcare, in connection with the use of digital technologies (regarding the encryption of medical data, control of access to information and proper authentication of users, conducting security audits of information systems to identify potential risks), which is necessary to eliminate potential threats to the security of medical information and violation of its confidentiality [28].

Ensuring the confidentiality of medical information, as noted by P.S. Krakhmalov and H.V. Mulyar, is one of the basic principles that contributes to the protection of patients' rights and increases the level of trust in both medical professionals and the health care system as a whole. Without a doubt, confidentiality is a fundamental component of the relationship between a doctor and a patient, and their relationship is based on mutual trust (the patient trusts the doctor if he acts in the best interests of the patient, and the doctor - when the pa-

tient is honest and provides him with all the necessary information to provide proper medical care) [29].

K. Horner and P. Burcher draw attention to the specifics of the trust relationship between the patient and the doctor in the case of the use of additional reproductive technologies, taking into account, first of all, that the surrogate mother must provide prior consent to the disclosure of confidential information about her (contractual waiver of confidentiality), and therefore her ability to be completely open and honest with her doctor in all cases (even regarding accidents or errors) is questioned, based on the fact that the doctor may indicate this in the medical documentation, and as a result, this may be the basis for legal liability for breach of the surrogacy contract. The physician should be aware that this may negatively impact his or her relationship with the patient (even before any misconduct by the patient occurs or without the physician disclosing confidential information) and the quality of care, as the surrogate mother may not provide important information necessary for her care during pregnancy [30].

The issue of the peculiarity of the relationship between the patient and the doctor was also investigated by O.S. Bilanov [31], noting that a person is most vulnerable at the moment when they seek medical help. In his opinion, one of the most vulnerable are patients who seek surrogacy services, since they share all personal information with the doctor regarding the health status of both the man and the woman, and therefore such relationships are based not only on trust, but also require medical professionals to have high moral and ethical standards and clear legal norms aimed at protecting information, based primarily on the need for constant exchange of information between all participants in the surrogacy relationship (biological parents, medical institution and surrogate mother of the child).

The individual's confidence in the confidentiality of one's personal and other medical data, as well as the existence of a trusting relationship, for example, between subjects of medical legal relations, are the determining conditions that encourage an individual to provide permission (informed consent) to receive and further process such data. Many owners of medical data, as scientists note, support the use of their data for research to improve the quality of medical services, at the same time, they are concerned about the possible violation of the confidentiality of their information or improper use or processing of data [32]. Providing an individual's medical data to support scientific research, medical innovations and other initiatives in the field of health care is a voluntary act. However, the provision of such data and their further processing in many cases faces significant difficulties, primarily due to issues of ensuring their confidentiality and security (the most critical concern is related to the potential risk that an individual can be further identified from their data [33]), so reliable guarantees for the protection of the rights of individuals who provide (grant) their medical data are extremely important [34].

The need for a balanced legislative mechanism for providing information and access to it, as well as ensuring the confidentiality of information about a person's health and other information that is a type of information about a person, O.A. Chaban considers as an important element of the implementation of online services and electronic health care, which are components of the development of cooperation and bringing our national legislation into line with European standards in the areas of information society development (Chapter 14) and public health (Chapter 22) [35] of the Association Agreement between Ukraine and the European Union. Cooperation in the field of public health primarily involves increasing the level of security in the field of health care as a prerequisite for sustainable development and economic growth of our state.

Cooperation in the exchange of health data, as well as ensuring their confidentiality and cybersecurity, are crucial conditions for ensuring respect for human rights (primarily in the area of privacy) and providing them with quality medical care. Such cooperation is important in any area of health care, but, as scientists note, in organ transplantation, effective data harmonisation is crucial due to the complex interaction of factors and the need for large, high-quality data sets for accurate analysis of results, which are constantly not only increasing but also improving [36]. It should be noted that the practice of data sharing in medical research is widely supported by governments around the world (including the European Commission, which considers «open access to publications and research data» as a cornerstone of its «Open Science» policy), as well as by numerous international organizations (e.g., the World Medical Association (WMA), the World Health Organization) and national institutions (in particular, the National Institute for Health and Care Research of the United Kingdom and the National Institute of Health of the United States), which proceed from the need for continuous improvement in the field of openness and transparency of research, as well as effective management and exchange of medical data [37].

Despite the huge potential of using various sets (bases) of medical data, primarily in the field of transplantology and the application of reproductive technologies, the following problematic aspects of their formation and application can be identified, namely: the complexity of developing and ensuring a reliable cybersecurity

infrastructure [25]; fragmentation and the presence of other shortcomings in the processes of data generation [36]; the need to ensure confidentiality and protection of personal data, for example, of donors and recipients [38]; the presence of various jurisdictional difficulties regarding the cross-border exchange of medical data [37], the insufficient level of digital literacy of all participants in medical legal relations and a number of other problematic aspects of their formation and application, which were investigated in more detail in one of our scientific works [39].

CONCLUSIONS

Given the continuous process of increasing the use of information and innovative technologies in the field of healthcare, as well as the increase in the volume of personal and other medical data of an individual (and the diversification of their types), it is becoming increasingly difficult to ensure confidentiality and proper protection of such information, primarily from unauthorized disclosure and possible further misuse.

Although the EU, the USA, and many other countries of the world have developed standards (regulations) for the protection of personal data and other confidential information of individuals, including in the field of healthcare, research in this area indicates the difficulty in implementing these standards in practice and the presence of cases of unauthorized collection and dissemination of such data about an individual. This is due, in particular, to the fact that the rapid development of the use of information technologies, especially in the field of healthcare, unfortunately leads to the emergence of new illegal ways of obtaining personal and other medical data of an individual, new manifestations of criminal acts, and based on the scale of the use of medical information, this problem is becoming global.

Despite positive trends in the field of transplantology and reproductive technologies, the problem of maintaining the confidentiality of personal and other medical data of all participants in medical-legal relations remains relevant. This issue is regularly studied by scientists, who usually emphasise the difficulty of achieving a compromise between the need to create large-scale databases with patients' medical information and the need to guarantee their confidentiality. Without a doubt, confidentiality is a fundamental component of the relationship between a doctor and a patient, and their relationship is based on mutual trust, especially in the field of transplantology and the use of additional reproductive technologies, which require medical professionals not only to clearly apply the norms of legislation in this area, but also to adhere to high moral and ethical standards of professional activity, taking into account, first of all, the need for permanent exchange of information between many participants in such special legal relations.

It is necessary to realize that cooperation in the field of exchange of medical data (especially in the field of transplantology and the use of additional reproductive technologies), as well as ensuring their confidentiality and cybersecurity are determining conditions in terms of ensuring compliance with human rights (primarily in the field of privacy) and providing them with high-quality medical care. In addition, a person's confidence in ensuring the confidentiality of their personal and other medical data, as well as the presence of trusting relationships, for example, between subjects of medical legal relations, are determining conditions that encourage a person to provide permission (informed consent) to receive and further process such data. Therefore, the issues of disclosing the essence of legal, organisational and technical methods of ensuring confidentiality and proper protection of medical information remain relevant.

REFERENCES

1. Zaborovskyy V, Ustych O, Popovych T, Manzyuk V. Certain ethical issues that arise when using 3D bioprinting technology. Wiad Lek. 2025;78(4):915-920. doi: 10.36740/WLek/203904. DOI
2. Zaborovskyy VV. Vyklyky ta perspektyvy zastosuvanni innovatsiynykh tekhnolohiy v sferi okhorony zdorov''ya (transplantolohiya i DRT) ta problemy zabezpechennya konfidentsiynosti medychnoyi informatsiyi u voyennyy chas [Challenges and prospects for the application of innovative technologies in the field of health care (transplantation and ART) and the problems of ensuring the confidentiality of medical information in wartime]. Analitychno-porivnyal'ne pravoznavstvo. 2025;2:545-552. doi: 10.24144/2788-6018.2025.02.81. (Ukrainian) DOI
3. Zaborovskyy V, Stupnyk Ya, Hetsko M, Chervko P. Legal conflicts in medical practice and methods of their resolution. Wiad Lek. 2023;76(11):2517-2524. doi: 10.36740/WLek202311128. DOI
4. Zaborovskyy VV, Stoyka AV. Deyaki yurydychni aspekty zastosuvannya tekhnolohiy virtual'noyi real'nosti v psykhoterapiyi [Some legal aspects of the use of virtual reality technologies in psychotherapy]. Zakarpat·s'ki pravovi chytannya: materialy KHII Mizhnarodnoyi naukovo-praktychnoyi konferentsiyi (m. Uzhhorod, 29-30 kvitnya 2020 roku). Uzhhorod: RIK-U. 2020, p.347-354. https://dspace.uzhnu.edu.ua/server/api/core/bitstreams/84e17aba-fc13-44c3-8a06-24e105dd3c75/content [Accessed 30 October 2025] (Ukrainian)
5. Schwab AP, Luu HS, Wang J, Park JY. Genomic privacy. Clin Chem. 2018;64:1696-1703. doi: 10.1373/clinchem.2018.289512. DOI

6. Gupta R, Iyengar R, Sharma M et al. Consumer Views on Privacy Protections and Sharing of Personal Digital Health Information. JAMA Netw Open. 2023. doi: 10.1001/jamanetworkopen.2023.1305. DOI
7. Dobbs v Jackson Women's Health Organization. US. 2022. https://www.supremecourt.gov/opinions/21pdf/19-1392_6j37.pdf [Accessed 30 October 2025]
8. Tighe J, Shand F, Ridani R et al. Ibobbly mobile health intervention for suicide prevention in Australian Indigenous youth: a pilot randomised controlled trial. BMJ Open. 2017. doi: 10.1136/bmjopen-2016-013518 pmid:28132007. DOI
9. Iribarren SJ, Cato K, Falzon L, Stone PW. What is the economic evidence for mhealth? a systematic review of economic evaluations of mhealth solutions. PLoS One. 2017. doi: 10.1371/journal.pone.0170581. DOI
10. EU General Data Protection Regulation. https://gdpr-info.eu/ [Accessed 30 October 2025]
11. Health Insurance Portability and Accountability. Act of 1996. https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996 [Accessed 30 October 2025]
12. US Food and Drug Administration. Guidance on the Postmarket Management of Cybersecurity in Medical Devices. 2016. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/ postmarket-management-cybersecurity-medical-devices/ [Accessed 30 October 2025]
13. Consumer Council of Norway. Out of Control. 2020. https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf [Accessed 30 October 2025]
14. Tangari G, Ikram M, Ijaz K et al. Mobile Health and Privacy: Cross Sectional Study. BMJ. 2021. doi: 10.1136/bmj.n1248. DOI
15. Spector-Bagdady K, Mello MM. Protecting the Privacy of Reproductive Health Information After the Fall of Roe v Wade. JAMA Health Forum. 2022;3(6). doi: 10.1001/jamahealthforum.2022.2656. DOI
16. Huyvan PD. Pravovi zasady zakhystu personal'nykh danykh [Legal principles of personal data protection]. Nauk. visn. Uzhhor. nats. un-tu. Seriya: Pravo. 2018;51(1):87-91. https://dspace.uzhnu.edu.ua/bitstreams/48e4ff4d-97cd-4c7e-b8fe-005262c48a12/download [Accessed 30 October 2025] (Ukrainian)
17. Omelchenko O. Zakhyst biobankamy personal'nykh danykh donoriv u konteksti pryntsypu vidkrytosti nauky [Omelchenko O. Protection of donors' personal data by biobanks in the context of the principle of open science]. Pidpryyemnytstvo, hospodarstvo i pravo. 2017;12:54-57. http://pgp-journal.kiev.ua/archive/2017/12/13.pdf [Accessed 30 October 2025] (Ukrainian)
18. Mulligan SP, Linebaugh CD. Data Protection Law: An Overview, Congressional Research Service. 2019. https://sgp.fas.org/crs/misc/R45631.pdf [Accessed 30 October 2025]
19. Musienko AV, Musienko VV. Aktual'ni aspekty normatyvno-pravovykh mekhanizmiv zakhystu personal'nykh danykh v elektronnykh medychnykh reyestrakh v Ukrayini [Current aspects of regulatory and legal mechanisms for protecting personal data in electronic medical registers in Ukraine]. Dictum Factum. 2022;1(11):17-22. https://df.duit.in.ua/index.php/dictum/article/view/213 [Accessed 30 October 2025] (Ukrainian)
20. Elektronnyy retsept v Ukrayini – pohlyad yurystiv [Electronic prescription in Ukraine – the view of lawyers]. 2019. https://www.legalalliance.com.ua/novini/elektronnij-recept-v-ukraini-poglad-uristiv/ [Accessed 30 October 2025] (Ukrainian)
21. Tully J, Selzer J, Phillips JP et al. Healthcare challenges in the era of cybersecurity. Health Secur. 2020;18(3): 228-231. doi: 10.1089/hs.2019.0123. DOI
22. Schneble ChO, Elger BS, Shaw DM. Google's Project Nightingale highlights the necessity of data science ethics review. EMBO Mol Med. 2020;12(3). doi: 10.15252/emmm.202012053. DOI
23. Ikeda S. Wave of cyber attacks hits US healthcare system as FBI warns of coordinated criminal campaign. Singapore: CPO Magazine. 2020. https://www.cpomagazine.com/cyber-security/wave-of-cyber-attacks-hits-us-healthcare-system-as-fbi-warns-of-coordinated-criminal-campaign/ [Accessed 30 October 2025]
24. Alder S. Judge Sets Deadline for Motions to Dismiss Claims in Change. Healthcare Data Breach Lawsuits. 2025. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/ [Accessed 30 October 2025]
25. Chirra DR. Mitigating Ransomware in Healthcare: A Cybersecurity Framework for Critical Data Protection. Revista de Inteligencia Artificial en Medicina. 2021;12(1):495-513.
26. US Healthcare at risk: Strengthening resiliency against ransomware attacks. 2024. https://www.microsoft.com/en-au/security/security-insider/emerging-threats/US-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks#footnoteref4 [Accessed 30 October 2025]
27. Yesimov SS. Zakhyst personal'nykh danykh u konteksti rozvytku dynamichnykh system [Personal data protection in the context of the development of dynamic systems]. Naukovyy visnyk derzhavnoho universytetu vnutrishnikh sprav. 2013;3:198-207. http://nbuv.gov.ua/UJRN/Nvlduvs_2013_3_25 [Accessed 30 October 2025] (Ukrainian)
28. Pishta VI. Zakonodavchyy analiz zakhystu medychnoyi informatsiyi u zv"yazku z vykorystannyam tsyfrovykh tekhnolohiy [Legislative analysis of the protection of medical information in connection with the use of digital technologies. Scientific Research and Innovation]. Scientific Research and Innovation: proceedings of the 2nd International Scientific and Practical Internet Conference, April 3-4, 2023. FOP Marenichenko V.V. Dnipro, Ukraine. https://dspace.uzhnu.edu.ua/items/7ef1335d-f859-441c-a499-19490908c58c [Accessed 30 October 2025] (Ukrainian)

29. Krakhmalov PS, Mulyar HV. Pravovi aspekty zabezpechennya konfidentsiynosti medychnoyi informatsiyi v Ukrayini [Legal aspects of ensuring the confidentiality of medical information in Ukraine]. Yurydychnyy naukovyy elektronnyy zhurnal. 2024;6:84-88. doi: 10.32782/2524-0374/2024-6/19 (Ukrainian) DOI
30. Horner C, Burcher P. A surrogate's secrets are(n't) safe with me: patient confidentiality in the care of a gestational surrogate. J Med Ethics. 2021;47(4):213-217. doi: 10.1136/medethics-2017-104518. DOI
31. Bilanov OS. Pravove rehulyuvannya medychnoyi tayemnytsi u dohovirnykh vidnosynakh surohatnoho meterynstva [Legal regulation of medical secrecy in contractual relations of surrogacy]. Aktual'ni problemy vitchyznyanoyi yurysprudentsiyi. 2022;4:18-23. https://repository.pdmu.edu.ua/500 [Accessed 30 October 2025] (Ukrainian)
32. Liu Y, Yang C, Liu Q et al. PDPHE: Personal Data Protection for Trans-Border Transmission Based on Homomorphic Encryption. Electronics. 2024;73(10):1-23. doi: 10.3390/electronics13101959. DOI
33. Voigt TH, Holtz V, Niemiec E et al. Willingness to donate genomic and other medical data: results from Germany. Eur J Hum Genet. 2020;28(8):1000-1009. doi: 10.1038/s41431-020-0611-2. DOI
34. Gaballah SA, Abdullah L, Alishahi M et al. Anonify: Decentralized Dual-level Anonymity for Medical Data Donation. Proceedings on Privacy Enhancing Technologies (PETS). 2024;3:94-108. doi: 10.56553/popets-2024-0069. DOI
35. Chaban OA. Pravo fizychnoyi osoby na tayemnytsyu pro stan zdorov"ya v Ukrayini [The right of an individual to confidentiality about health status in Ukraine]: dys. … kand. yuryd. nauk. Kyyiv, 2018:222 https://www.researchgate.net/publication/371206051_Pravo_fizicnoi_osobi_na_taemnicu_pro_stan_zdorova_v_Ukraini [Accessed 30 October 2025] (Ukrainian)
36. Hosseini SA, Kazemzadeh R, Foster BJ et al. New Tools for Data Harmonization and Their Potential Applications in Organ Transplantation. Transplantation. 2024;108(12):2306-2317. doi: 10.1097/TP.0000000000005048. DOI
37. Hammond-Browning N, Williams NJ. Ethical data management and sharing in uterus transplantation – reflections and recommendations. International Legal and Ethical Perspectives on Uterus Transplantation. Elgar Studies in Health and the Law Cheltenham. 2024. doi: 10.4337/9781803920498.00021. DOI
38. Chornenka DS. Biomedychni ta etychni pryntsypy transplantatsiyi v konteksti zakhystu prav lyudyny ta zastosuvannya Konventsiyi OV"YEDO [Biomedical and ethical principles of transplantation in the context of human rights protection and application of the Convention on the Elimination of All Forms of Discrimination against Women]. Naukovyy visnyk Uzhhorods'koho Natsional'noho Universytetu. Seriya PRAVO. 2023;80(1):141-150. doi: 10.24144/2307-3322.2023.80.1.20. (Ukrainian) DOI
39. Zaborovsky VV. Problemni aspekty formuvannya ta zastosuvannya medychnykh baz danykh v umovakh tsyfrovoyi transformatsiyi sfery okhorony zdorov"ya [Problematic aspects of the formation and application of medical databases in the context of digital transformation of the healthcare sector]. Innovative Research in Science and Economy: Collection of Scientific Papers with Proceedings of the 1st International Scientific and Practical Conference (Brussels (Belgium), July 30 – August 1, 2025). Brussels: International Science Unity. 2025, pp.108-110. https://isu-conference.com/wp-content/uploads/2025/07/Brussels_Belgium_30.07.25.pdf [Accessed 30 October 2025] (Ukrainian)

CONFLICT OF INTEREST

The Authors declare no conflict of interest

CORRESPONDING AUTHOR:
Viktor V. Zaborovskyy
Uzhhorod National University
14 Universytetska St, 88000 Uzhhorod, Ukraine
e-mail: zaborovskyviktor@gmail.com

ORCID AND CONTRIBUTIONSHIP

Viktor V. Zaborovskyy: 0000-0002-5845-7535 A B D
Vasil V. Manzyuk: 0000-0003-2133-1573 B D
Vasil P. Fennych: 0000-0003-2649-1322 F
Stanislav V. Shchoka: 0000-0002-7165-2191 B D

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

RECEIVED: 02.12.2025
ACCEPTED: 10.02.2026