MEDICINE, LAW & SOCIETY
Vol. 17, No. 1, pp. 153–170, April 2024

DIGITAL TRANSFORMATION OF HEALTH: TOWARDS THE EUROPEAN HEALTH DATA SPACE

Accepted
28. 2. 2024

Revised
17. 3. 2024

Published
18. 4. 2024

MAJA PROSO
University of Split , Faculty of Law, Split, Croatia
maja.proso@gmail.com

CORRESPONDING AUTHOR
maja.proso@gmail.com

Abstract The European space for health data (EHDS) is the first European proposal for the arrangement of a specific area common to the entire EU. The main goals are enabling citizens to control and use their own health data, nationally and throughout the EU (primary use of health data), cross-border exchange of health data and building a single market for digital health services. A further goal is to create an effective legal framework for the use of health data for research and innovation purposes (secondary use of health data), as well as the establishment of electronic health records and the development of a health data management system. In the paper author presents the concept of health data privacy in digital age and analyses the current health data protection legal framework. The paper examines the provisions of the EHDS Proposal, critically analysing the proposed terms of primary and secondary use of health data, as well as it's rules on data portability and interoperability.

Keywords
data protection,
European space for health dana,
health data,
primary use of health data,
secondary use of health data

https://doi.org/10.18690/mls.17.1.153-170.2024

1 Introduction

Modern information and communication technology enables healthcare providers to access their patients' data faster and easier. A drawback of modern technology is that it may pose a danger to individuals' privacy, especially in relation to the processing, use and exchange of their personal data. This especially applies to the patient's health data, which is highly sensitive. To ensure the protection of health data, it is essential to store patient data using reliable digital systems. The fundamental goal of digital health information systems is to protect the confidentiality, availability and integrity of patient health data.

The protection of personal data is guaranteed by numerous international and national legal documents. A major step forward in the field of data protection was the adoption of the General Data Protection Regulation (hereinafter: GDPR) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals in connection with the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC in 2018. Pursuant to the GDPR, the fundamental goals of personal data protection (health data included) are to both maximally protect the privacy of citizens and the flow of such data. Under GDPR, health data denotes all data relating to the previous, current and future physical and mental health of an individual, including the number and identifier assigned for unique identification for health purposes and other information collected during registration and providing health care services to the patient. Health data also includes a number, symbol or label assigned to an individual for the purpose of their unique identification for health purposes, as well as information derived from testing or examination of a body part or body substance, among others from genetic data and biological samples, and any information about, for example, a person's disease, disability, risk of disease, medical history, clinical treatment, or physiological or biomedical condition regardless of its source, such as from a physician or other health care professional, a hospital, a medical device, or an in vitro diagnostic test (Recital 35 GDPR).

The processing of health data should be performed while preserving the interests, fundamental rights and dignity of the individual, with the provision of measures aimed at reducing the risk of misuse as well as of all illegal, unjustified access and use, and sanctioning the illegal use and misuse of this category of personal data. In the European Union, as far as the use of digital health data is concerned, citizens are still faced with numerous difficulties in controlling their own digital health records. Moreover, most of the EU member states have not yet developed the necessary interoperable systems that would enable the voluntary cross-border sharing of health data.

In 2022, the European Commission published "Communication: European space for health data and exploiting the potential of health data for citizens, patients and innovations". That document, along with the Communication of the published Proposal, contains the main guidelines of the Regulation for the European Health Data Area (hereinafter: EHDS). Within the Framework of the European strategy for data, the establishment of common European data areas in specific areas of activity was proposed, and the EHDS is the first such European proposal for the arrangement of a specific area common to the entire EU.

The main goals of establishing the EHDS are to enable citizens to control and use their own health data, nationally and throughout the EU (the so-called primary use of health data), to enhance the cross-border exchange of health data and to build a single market for digital health services. Further goals of the EHDS are to create an effective legal framework for the use of health data for research and innovation purposes (the so-called secondary use of health data), to establish electronic health records, and to develop a health data management system. In the paper, the author analyzes both the concept of health data privacy in the digital age and the current health data protection legal framework. The paper examines the provisions of the proposed EHDS, critically analysing the proposed terms of primary and secondary use of health data, as well as rules on data portability and interoperability.

2 Digital Transformation of Health

2.1 Privacy of health data in the digital age

Subsumed within the patient's right to privacy are the right to confidentiality and privacy of personal data about health, medical status, family circumstances, the course of treatment itself and prognosis of treatment outcomes, as well as all other relevant data. The right of individuals to protect their personal data, including health data, derive both from Article 16(1) of the Treaty on the Functioning of the European Union (TFEU)[1] and Article 8 Charter of the European Union on Fundamental Rights[2], and until the beginning of the 21st century was equated with the right to privacy in legal doctrine. The underlying purpose of the basic regulations related to the right to data protection was to protect individuals' right to privacy in this context. Moreover, in as many as eight Recitals, Directive 95/46/EC referred to the fundamental rights and freedoms of individuals, and the special right to privacy, which implies that the European legislator's intent at the time was not to protect the personal data of a person as such, but to protect the data in order to protect the human right to privacy (Bukovac, Puvača & Demark, 2019, p. 292). With the entry into force of the Charter, a clear demarcation was made at the normative level, making their legal protection independent (Bukovac, Puvača & Demark, 2019, p. 292).

According to some authors, three main elements justify separating the right to privacy from the right to personal data protection (Štareikė & Kausteklytė Tunkevičienė, 2021, p. 239). First, data protection clearly protects values that are not at the heart of the concept of the right to privacy, such as regularity of treatment, legality, and consent of the person to process personal data. Another reason for separating and recognizing the right to data protection as an independent right is to respect the different constitutional traditions of

[1] *„Everyone has the right to the protection of their personal data."*

[2] *„1. Everyone has the right to the protection of personal data relating to him or her. 2. Such data must be processed fairly, for established purposes and based on the consent of the person concerned, or on some other legitimate basis established by law. Everyone has the right to access collected data relating to him or her and the right to correct it. 3. Compliance with these rules is subject to the supervision of an independent body."*

Europe. Third, the need to protect personal data has increased, especially in response to new challenges stemming from information technology, so it was no longer appropriate to attribute these new challenges and problems to privacy violations (De Hert & Gutwirth, 2006).

The right to privacy and the protection of personal data are closely related, sometimes they overlap, but they are not identical rights (although they defend similar values – human dignity, the right to autonomy, secrecy of private life, etc.) (Štareikė & Kausteklytė Tunkevičienė, 2021).

One violation can simultaneously violate both rights (Milaj, 2020). The consequences of the violation of the right to the protection of personal data are often manifested as a violation of the right to the privacy of personal and family life. The jurisprudence of the European Court of Human Rights (hereinafter: ECtHR), precisely based on Article .8 of the European Convention on Human Rights on the right to respect for private and family life, provides protection in cases of violation of personal data, including patient health data. The case law of the ECtHR raises the topic of existence of a legal basis for the transfer of patient data to any entity. The security of patients' personal data and eliminating security risks are also of great importance and for medical service providers imply the immediate application of the GDPR (Apan, 2021, p. 9). The reason for the special status of health data is that health and genetic data belong to the "private" sphere of the person (respondent), since they relate to their most intimate personal areas. Therefore, the unauthorized disclosure of this data is potentially intended to cause discrimination and stigmatization in the domains of personal, professional or social life of individuals (Lobato de Faria & Valente Cordeiro, 2014, p. 124).

Data protection rules are the "practical" or "feasible" part of protecting the right to privacy and confidentiality of health information. This is particularly relevant currently, because respect for these rights depends almost entirely on the existence of a very objective security measure in health information

technologies (IT sector) (Lobato de Faria & Valente Cordeiro, 2014). The growth of information technology has led to the increased use of health information for purposes other than those for which it was originally collected.

Presently, healthcare practice generates data exchanges and stores huge amounts of patient-specific information (Beck & Gollapudi, 2012). This generation of electronic health data holds great promise not only to significantly contribute to healthcare provision but also to transform biomedical research (Coorevits, 2013, pp. 547–560). Electronic health records incorporate a vast amount of patient information and diagnostic data, most of which is considered protected health information. With advances in technology, the emergence of advanced cyber threats has escalated, which hinders the privacy and security of health information systems (Kruse & Smith, 2017, p. 127). The use of personal health information for commercial gain has also become increasingly common (Prudnykova, 2021, p. 146).

2.2 Health data regulatory framewework

The patient can easily be harmed either by unauthorized or illegal collection and storage of personal health data, as well as by the disclosure of medical secrets, which in the grossest way violates the patient's right to privacy, thereby violating the relationship of trust between the patient and the health provider. Under GDPR, the previous regulations pertaining to the protection of personal data in the EU were uniquely regulated for all member states, with common principles for processing personal data, the rights of data subjects, the obligations of managers and processors, and defined sanctions for violators. Data on the patient's state of health undoubtedly belong to personal data and must not, as a rule, be disclosed to third parties, and the rules on their protection must be respected by all subjects (Jelenc Puklavec, 1998).

The judgment of the European Court from 2015 explains that it follows from judicial practice that the expression "data concerning health" should be broadly interpreted to include data on all physical and mental aspects of a person's health. However, this term should not be extended to include expressions that do not lead to the disclosure of any information about a person's health or state of health (Bevanda & Čolaković, 2016, p. 147).

According to the Act on Data and Information in Health Care, health data is information about an individual, about their physical or mental health, including the health services provided to them in the health system of the Republic of Croatia.

Data on the state of health are also protected by the rules on medical confidentiality. Medical confidentiality is one of the most effective instruments for protecting the patient's privacy, i.e. protecting the confidentiality of information about their health. As a rule, it is considered that medical secrecy includes only the facts that the doctor learns in the course of their vocation, mostly from the patient and in connection with the treatment provided (Čizmić, 2008, p. 17). The obligation to maintain medical confidentiality applies particularly to the confidentiality of medical documentation about the patient, because it is the documentation that contains information about the patient's state of health. TMaintaining medical confidentiality also extends to IT systems in which data are stored.

Medical documentation consists of medical records and documents created in the process of providing health care by authorized health care providers that contain information about the health status and course of treatment of patients. Medical documentation includes any document created in a healthcare facility, signed by a healthcare worker, usually a doctor (Čukić, 2002, p. 260). Medical documentation has multiple purposes. Medical documentation helps enable medical providers to render proper treatment to their patients and to advance scientific research, so it must be guided in such a way that it can, at any time, provide other doctors and the patient with

accurate information about the diagnostic and therapeutic measures taken (Čizmić, 2009, p. 94). A doctor or other responsible person who performs health care activities therefore has the duty to secure medical documentation stored on electronic media against alteration, premature destruction or unauthorized use.

However, not all facts that a doctor learns from a patient constitute secrets. Secrecy extends only to those findings and circumstances that intrude on the patient's interests or intimate feelings in such a way that the patient does not want to disclose them to other people or because their disclosure would harm the patient. Whether a disease will be considered a medical secret depends, for example, on whether, according to the understanding of society, this disease is considered shameful, which reduces the status and reputation of the patient in the eyes of the community (Čizmić, 2008, p. 24).

The right to confidentiality of data related to the patient's state of health derives from the right to personality, which protects the patient's personality by various means, since human personality falls into not only a psychological category, but also constsitutes a legal concept (Radolović, 2006, p. 133). Older legal literature emphasized that the protection of personal data is one of the subtypes of the protection of personality rights. The purpose of personal data protection is to ensure the realization and protection of private life (right to privacy) and other human rights and fundamental freedoms in the collection, processing and use of personal data.

Data related to an individual's health fall into a special category of personal data that needs additional protection. Such data is a very sensitive category of data, the unjustified publication of which may cause damage to the person whose health data has been published. Pursuant to Article 5 of the GDPR, personal data must be processed lawfully, fairly and transparently with respect to the data subject, collected for specific, explicit and lawful purposes, appropriate, relevant and limited to what is necessary in relation to the purposes for which they are processed , accurate and, if necessary, up-to-date.

Concerning the processing of special categories of personal data (such as health data), there must also be exceptions to the principled ban on the processing of special categories of personal data from Article 9(2) of the GDPR.

According to the Health Care Act, health workers are obliged to keep medical documentation and other records on the persons to whom they provide health care. They are also required to submit a report on this to the competent health institution in accordance with the law governing the field of data and information in health care, and to provide information about their work at the request of the competent authority.

3 Towards the European Health Data Space

3.1 What is EHDS, in short?

The EHDS is the first common EU data space in a specific area to emerge from the EU strategy for data and is an integral part of the European Commission's digital transition priority. The EHDS Proposal introduces security criteria for electronic health record systems, in addition to it's interoperability. It builds upon the GDPR supporting the use of health data not only for diagnosis and treatment, but also for research, statistics or for public interest, such as protecting against serious cross-border threats to health, ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices (European Commission, A European data strategy, 2020). According to the European Commission, EHDS will provide immediate and easy access to data in electronic form, free of charge, allowing sharing with health professionals across the EU to improve health care delivery. Access will be granted only if the requested data are to be used for specific purposes, in closed, secure environments, and without revealing the identity of the individual (Horgan & Hajduch, 2022, p. 3).

3.2 The relationship of the EHDS Proposal with other legal acts in the field of digital health data protection

EHDS is designed to complement other EU legislation, because it builds further on the GDPR, the proposed Data Governance Act, the draft Data Act and the Network and Information Systems Directive. A significant difference, however, is that the EHDS applies to a specific sector, whereas the other EU data legislation to date is all generic, with provisions taking on a horizontal character (Hansen & Wilson, 2021) likely to be augmented with legislation on artificial intelligence and cybersecurity (Horgan & Hajduch, 2022, p. 3). As horizontal frameworks, they provide rules that also apply to the health sector. However, the EHDS contains more specific rules, cognizant of the sensitive nature of health data. EHDS relies on regulations such as GDPR, Regulation (EU) 2017/745 on medical devices, Regulation (EU) 2017/746 on in vitro diagnostic medical devices and the Cross-Border Healthcare Directive. It also allows the use of electronic health data for scientific or historical research, for official statistical purposes and for the public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and medicines or medical products. Within the legal framework of the EHDS, additional provisions are foreseen to promote interoperability and strengthen the right of individuals to data portability within the health sector.

3.3 Primary use of health data

To implement compatible digital health systems, interoperability requirements are necessary to enable cross-border data exchange between health-care information technology systems and health-care professionals (Raab et al., 2023, p. 841). The personal electronic health data definition contained in EHDS builds on the GDPR definition and it means data concerning health and genetic data as defined in GDPR, as well as data referring to determinants of health, or data processed in relation to the

provision of healthcare services, processed in an electronic form. The EHDS regulates these requirements for the EU in the context of two main use cases of electronic health data: primary use and secondary use (Raab et al., 2023).

Primary use of electronic health data means the processing of personal electronic health data for the provision of health services, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social security, administrative or reimbursement services (Article 2 EHDS). Articles 3 – 13. EHDS regulate primary use, which is the processing of personal electronic health data aiming to provide direct healthcare to the data subject. It is connected to the rights to access and receive information, rectification and data portability under the GDPR, building on these rights. Article 3 EHDS guarantees immediate electronic access to health data for individuals withot any fees.

The proposed definition of personal electronic health data aimed for primary use is broad and includes all "data referring to determinants of health". This expansive definition widens immensly the scope of data that can be collected (for example, data such as patients income, housing, nutrition habits etc.) This scope is, in our opinion, too wide and the proposed definition of personal electronic health data should be narrower and more precise in order to reduce the risk of possible unlawful primary use of health data.

3.4 Secondary use of health data

The secondary use of health data denotes health data processing for innovation, scientific research and other similar purposes. The minimum categories of data for secondary use are found in Article 33 EHDS. These are data impacting health, genetic data, health data registries, and clinical trials data. EHDS also defines purposes that are permited, which includes development and innovation activities (Article 34 EHDS), together with that are prohibited, which includes using data detrimentally against persons, advertising or marketing, or providing data access to third parties outside of

the permit, and developing products harmful to individuals (Article 35 EHDS).

A data user, in the context of secondary use of health data, can be any person with lawful access to electronic health data for secondary use. A data holder can be, according to EHDS, any entity in the field of healthcare and research or any EU institution, body or agency that has the right to make data available according to EU law. To be able to use health data, the data user must submit a request for access to health data, the modalities of which depend on the data in question (Articles 45 & 47 EHDS). These requests are assessed by the health data access body, who is responsible for giving access permission and deciding compatibility with the purposes listed in Article 34(1) EHDS.

EHDS relies to the GDPR setting the principles for lawful processing, which focuses on Articles 6 and 9, with the legal basis for secondary use grounded in Article 9(2)(g)-(j). Data users must demonstrate compliance with Article 6(1)(e) or (f), which requirs that access to data must be necessary to either perform a task in the public or some other legitimate interest. Data holders, in concordance with Article 6(1)(c) GDPR, must disclose this information to health data access bodies. Those who wish to reuse health data must apply to a health data access body for a permit. The data permit sets out how the data may be used and for what purpose. The data can only be accessed and processed in closed secure environments to be provided by the health data access bodies. The user who applied for the permit can onlyextract anonymous data from the secure processing environment.

If researchers, companies or public institutions need access to personal electronic health data, they can only access it in pseudonymised form, i.e. data offering information about the disease, symptoms and medication, without revealing the identity of the individual.

Use of the data to take decisions detrimental to individuals, to increase insurance premiums, to market health products towards health professionals or patients or to design harmful products or services will be forbidden. In

addition, data users must make public the results of their electronic health data uses and inform the health data access bodies of any significant findings relevant for the health of individuals.

The EHDS Proposal does not grant the possibility to opt out from having data used for secondary purposes. Also, the purposes for secondary use of health data foreseen in the EHDS, in our opinion, are too broad and can negatively result in sensitive health data being exploited for commercial purposes. A serious drawback of the Proposal is that it fails to contain any specific obligations to ensure that the requirements of anonymisation or pseudonymisation will be protected. This is particularly dangerous because genetic data, for example, cannot be anonymised and can reveal persons' personal data, for example, specific health issues, ethnic origin etc. Also, prohibitions on specific forms of secondary use of health data (such as marketing and advertising purposes) should have been, in our opinion, included in the EHDS Proposal.

3.5 Data portability and interoperability

The GDPR defines the right to data portability in Article 20(1). It provides that individuals have the right to receive their personal data in a clear, easy way, and to send these data to another controller without any hindrance from the original controller. The right to data portability, under the GDPR provisions, applies only with consent or contract. The right to data portability is regulated in EHDS, Article 3(8) and is closely linked to the primary use of health data. According to the definition of "electronic health data" and Recital 12 of EHDS, primary data portability, unlike GDPR, covers inferred data as well. Based on Recital 12 EHDS, health data processed under any of the legal bases for processing in line with Article 9 GDPR will fall under the right to portability.

The right to data portability is closely related to the concept of interoperability. Interoperability denotes the ability of different information systems to exchange and use health data effectively and efficiently. EHDS

has set strict requirements that are focused on electronic health record (hereinafter: EHR) systems. These requirements promote interoperability and data portability, in a way that provides data subjects more control over their health data. On one hand, interoperability promotes efficiency and inter-organisational alignment, but usually comes with privacy compromises, since access to health data becomes more comprehensive and longitudinal. On the other hand, strong privacy protections can enable interoperability while respecting the privacy of the individuals. For example, the DP-3T team demonstrated during the Covid-19 pandemic that one can build an interoperable infectious disease exposure notification system without necessarily compromising people's privacy. Yet, the issue of privacy and data protection is scarcely mentioned in the essential requirements and common specifications for the conformity declaration of the EHR systems' manufacturers (Terzis & Santamaria Echeverria, 2023). Lack of interoperability would result in inevitable restriction of data portability. Such restriction would consequently impede health systems from providing effective treatment for patients. EHDS aims to address such a possible negative outcome by setting stricter requirements for EHR systems to promote interoperability, portability and their interconnection.

4 Conclusion

Digitalisation is essential for the future of healthcare. However, the complexity and divergence of rules, structures and processes within and across EU member states makes it difficult to easily access and share health data. This creates barriers to healthcare, leaving patients unable to benefit from its potential. In essence, today's EU health sector is rich in data, but poor in making it work for people and science. (Communication from The Commission to The European Parliament and The Council: A European Health Data Space: harnessing the power of health data for people, patients and innovation, 2022., p. 1).

The recent COVID-19 pandemic has highlighted the importance of enabling and making digital health services more widely available. Although medical digital records are constantly improving, they also raise considerable concern about privacy, security, and confidentiality especially relating to highly sensitive information about health status. The proposed EHDS builds upon GDPR rules concerning the use of health data. It aims to further improve individuals' access to and to assert control over their digital health data, enabling certain health data to be reused for research and innovation purposes.

The complexity of the rules and procedures regarding the creation, storage, use and exchange of digital health data between EU member states makes it difficult for EU citizens to realize the full potential of digital transformation in relation to the use and protection of health data. Due to the present lack of interoperability in different EU member states, health professionals in many cases cannot access the entire medical records of patients, severely handicapping their ability to make proper diagnoses and decisions related to patient treatment, which in turn also imposes significant, additional costs to the health system and individuals and can lead to worse health outcomes for individuals. Lack of interoperability also causes significant administrative burden to healthcare professionals due to the need to manually enter or copy patient health data from one electronic system to another. In conclusion, for EHDS to be a fully functional and trustworthy tool, able to achieve its primary goal- to simplify and improve management of the patients health data across Europe - the key is to ensure interoperability between the health systems in all EU member states.

Acts, cases

Act on data and information in healthcare, Official Gazette no. 14/19.
Code of Medical Ethics and Deontology, Official Gazette No. 139/15.
Communication from the Commision to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM/2020/66 final.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016.
Directive 2011/24/EU of the European Parliament and the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011.
Directive of the European Parliament and the Council of October 24, 1995 on the protection of individuals in connection with the processing of personal data and on the free flow of such data OJ L 281, 23.11.1995.
European Commission Strasbourg,Communication from The Commission to The European Parliament and The Council A European Health Data Space: harnessing the power of health data for people, patients and innovation, 3.5.2022.COM(2022) 196 final.
European Commission, Strasbourg, 3.5.202, COM(2022) 197 final 2022/0140 (COD), Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Area, Legislative Financial Statement, p. 103.
European Commission (2020). A European data strategy, 2020. Retrieved from: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en, p. 1 (14 March 2024).
Health Care Act, Official Gazette no. 100/18, 125/19, 147/20, 119/22, 156/22.
Judgment CN v. European Parliament, T-343/13, ECLI:EU:T:2015:926.
Penal Code, Official Gazette no. NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23.
Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final.
Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final.
Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and on the repeal of Directive 95/46/EC (General Data Protection Regulation), OJ EU L119.
Regulation (EU) 2017/745 of the European Parliament and the Council of April 5, 2017 on medical products, amending Directive 2001/83/EC, Regulation (EC) no. 178/2002 and Regulation (EC) no. 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC OJ L 117/1, 5/5/2017.
Regulation (EU) 2017/746 of the European Parliament and of the Council of April 5, 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, OJ L 117/176, 5 5. 2017. Zakon o liječništvu, Narodne novine br. 121/03, 117/08.
Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, OJ 306 of 17 December 2007, Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, OJ C of 19 May 2008.

References

Apan, D.R. (2021). Personal Data Protection in Health: A Perspective of the European Court of Hurman Rights, *Journal of Law and Public Administration,* VII(13), 9.
Baretić, M. (2006). Pojam i funkcije neimovinske štete prema novom Zakonu o obveznim odnosima, *Zbornik Pravnog fakulteta u Zagrebu*, 56, 461- 500.
Beck, T., Gollapudi, S. et al. (2012), Knowledge engineering for health: a new discipline required to bridge the "ICT gap" between research and healthcare, *Human Mutation,* 33(5), 797-802, https://doi.org/10.1002/humu.22066
Bevanda, M. & Čolaković, M. (2016). Pravni okvir za zaštitu osobnih podataka u vezi sa zdravljem u pravu Europske unije, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 37(1), 147.

Bukovac Puvača, M. & Demark, A. (2019). Pravo na zaštitu osobnih podataka kao temeljno pravo i odgovornost za štetu zbog njegove povrede, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 40(1), 292.

Bukovac Puvača, M. (2015). Deset godina nove koncepcije neimovinske štete, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 36(1), 157 – 180.

Coorevits, P., Sundgren, M. et. al. (2013). Electronic health records: new opportunities for clinical research *(*Review*) Journal of Internal Medicine*, 547–560.

Čizmić, J. (2008). Pravo pacijenata na obaviještenost s posebnim osvrtom na zaštitu tajnosti podataka o zdravstvenom stanju pacijenta, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 29(1), 17.

Čizmić, J. (2009). Pravo na pristup podacima u medicinskoj dokumentaciji, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 30(1), 94.

Čukić, D. (2002). Pravo na medicinsku istinu preko medicinske dokumentacije – teškoće, greške, predlog mjera za njihovo otklanjanje, *"Pravni život*", LI(9), 260.

De Hert, P. J. A. & Gutwirth, S. (2006). Privacy, data protection and law enforcement: Opacity of the individual and transparency of power, in: Claes, E. & Duff, A. (Eds.), *Privacy and the criminal law,* 61-104.

Horgan, D., Hajduch, M. et al. (2022). European Health Data Space—An Opportunity Now to Grasp the Future of Data-Driven Healthcare. *Healthcare* 10, 3.

Jelenc Puklavec, A. (1998). Zdravstvena dokumentacija, zasebnost in kazenski postopek, *Zbornik "Medicina in pravo"*, god. 1996-1998, Maribor, 219-220.

Kruse, C.S. & Smith, B. et al. (2017). Security Techniques for the Electronic Health Records. *The Journal of Medical Systems*, 41, 127.

Lobato de Faria, P. & Valente Cordeiro, J. (2014). Health data privacy and confidentiality rights: Crisis or redemption?, *Revista portuguesa de saude publica*, 32 (2), 124.

Milaj, J. (2020). Safeguarding Privacy by Regulating the Processing of Personal Data – An EU Illusion?, *Euopean Journal of Law and Technology*, 11(2), doi/10.1093/idpl/ipaa025/6246144?searchresult=1

Prudnykova, O. et al. (2021). European Court of Human Rights as a Guarantee of Observation the Medical Secrecy, *The Journal of Forensic Science and Medicine*, 7(4), 146.

Raab, R. et al. (2023). Federated electronic health records for the European Health Data Space, *The Lancet, Digital Health*, 5(11), e841-e847.

Radolović, A. (2006). Pravo osobnosti u novom Zakonu o obveznim odnosima*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 27(1), 133.

Radolović, A. (2013). Specifični postupovno pravni problemi u zaštiti prava osobnosti*, Zbornik Pravnog fakulteta u Zagrebu*, 63(3-4), 695 – 715.

Štareikė, E. & Kausteklytė-Tunkevičienė, S. (2021). Health Data Protection as a Measure of Realizing an Individual's Right to Privacy, *Public security and public order*, (26), 239.

Terzis, P. & Santamaria Echeverria, O.E. (2023). Interoperability and governance in the European Health Data Space regulation. *Medical Law International*, 23(4), 368-376. https://doi.org/10.1177/09685332231165692

Povzetek v slovenskem jeziku

Evropski prostor za zdravstvene podatke (EHDS) je prvi evropski predlog za ureditev specifičnega področja, skupnega celotni EU. Glavni cilji so omogočiti državljanom nadzor nad lastnimi zdravstvenimi podatki ter njihovo uporabo na nacionalni ravni in po vsej EU (primarna uporaba zdravstvenih podatkov), čezmejna izmenjava zdravstvenih podatkov in izgradnja enotnega trga za digitalne zdravstvene storitve. Nadaljnji cilj je ustvariti učinkovit pravni okvir za uporabo zdravstvenih podatkov v raziskovalne in inovacijske namene (sekundarna uporaba zdravstvenih podatkov) ter vzpostavitev elektronskih zdravstvenih zapisov in razvoj sistema za upravljanje z zdravstvenimi podatki. V članku je predstavljen koncept zasebnosti zdravstvenih podatkov v digitalni dobi, nadalje pa prispevek analizira trenutni pravni okvir za zaščito zdravstvenih podatkov. Članek preučuje določbe Predloga EHDS, kritično analizira predlagane pogoje za primarno in sekundarno uporabo zdravstvenih podatkov, kot tudi pravila o prenosljivosti podatkov in interoperabilnosti.