

Review**HEALTH DATA DIGITIZATION IN SERBIA AND THE RISK OF MISUSE****Jasmina M. Veličković¹, Mitar Lutovac², Mia Jokić³**¹Medika College of Vocational Studies in Healthcare²Faculty of Management, Union University “Nikola Tesla” Belgrade³European Business School, Belgrade, Serbia**Received:** March 17, 2025; **Revised:** June 15, 2025; **Accepted:** June 20, 2025**Published:** June 26, 2025**DOI:** 10.5937/annnur3-5758**Abstract**

The use of digital technologies in healthcare delivery has become increasingly prominent in recent years. Information and communication technologies contribute to greater efficiency in the health system and improved access to healthcare, as well as offering financial benefits. Digital health encompasses a wide range of services, such as electronic health and mobile health, but also includes emerging research areas like the application of artificial intelligence, big data, and genomics. As the population ages and the burden of non-communicable diseases increases, pressure on health systems will intensify, underscoring the need to implement both existing and new technological solutions. However, digitization also raises numerous issues, including data protection and privacy concerns, changes in traditional communication and interactions between doctors and patients, and new forms of consent enabled by digital technologies. This paper presents the current state of digital health development and examines development trends and the potential for data misuse in the Republic of Serbia.

Keywords: health, healthcare, electronics, records, patient rights**Corresponding Author:** Jasmina M. Veličković, e-mail: jasminav.frad@gmail.com

Introduction

The constant advancement of information technologies has led to their integration into various aspects of individuals' lives, aiming to provide as many high-quality services as possible to ease everyday life for users. The health system, as a subsystem of the social system, has the primary task of improving and preserving human health. According to the World Health Organization, the health system includes a health infrastructure that offers a range of programs and services, delivering healthcare to individuals, families, and communities.

Modern technological infrastructure—such as the internet and smartphones with built-in sensors—is accessible to a large portion of the population. This enables the collection of significant amounts of user-related data, which can be used to enhance the quality and availability of healthcare services. Information and communication (IC) technologies are already being implemented within healthcare systems, regardless of broader concepts.

Personal data refers to information relating to an identifiable person—either directly or indirectly—through identifiers such as names, identification numbers, location data, or characteristics of physical, physiological, genetic, economic, cultural, or social identity. The right to privacy and protection of patients' personal data is especially significant in today's globalized, digitally connected world. Safeguarding patient privacy is fundamental to upholding citizens' rights. It is essential to determine the scope of this protection and establish a balance between the legitimate interests of third parties, society, and the state on the one hand, and the interests of the individual—the patient—on the other. Recent changes in European and Serbian legislation regarding personal data protection are a key reason for analyzing this issue, which is relevant both legally and medically.

Healthcare services provided for different purposes must be legally regulated to prevent arbitrary decisions by service providers. Confidentiality forms the basis of the doctor–patient relationship, which has shifted from a

paternalistic model to one based on partnership. This trust is crucial for the effective provision of medical services. Ensuring the confidentiality of patient health information is both a legal obligation of healthcare providers and a fundamental right of patients. The inalienable right to privacy and confidentiality of health data is closely linked to personal data protection—both are mutually dependent and guaranteed by the Constitution. These rights must be legally protected, especially when data is being processed.

Over the past 30 years, the development of information technology has drastically increased the volume of data collected on individuals. Modern lifestyles, digital communication, global cooperation, and online transactions have necessitated comprehensive regulations regarding the classification, collection, processing, and storage of personal data. Digitization in healthcare brings many opportunities for improved and more accountable medical services for individuals. However, it also introduces risks that may compromise privacy and personal data protection. Health-related personal data is critical in the digital world—without it, e-health could not exist, develop, or adapt to ongoing changes in society and technology. Digitization in healthcare involves using modern ICT (information and communication technologies) to meet the needs of citizens, patients, healthcare professionals, service providers, and policymakers. Health is a universal concern; thus, improving healthcare systems benefits the entire population, as everyone has the right to appropriate and affordable medical services.

The implementation of information and telecommunication technologies in medicine enhances the efficiency and quality of medical and administrative processes managed by institutions, professionals, patients, insurers, and the government, with the ultimate goal of improving patient health. Health data is accessible regardless of where the patient, healthcare provider, or data storage system is located. The patient is considered the sole owner of this information. Physicians, medical institutions, insurers, and the state are authorized to access the data only to the extent

necessary to fulfill their duties—and only with the patient's explicit consent. Patients have the right to request and receive their health data in electronic form. Doctors and healthcare providers may use this information solely for the specified purpose. The internet also empowers patients by giving them access to information about their conditions, treatment options, healthcare providers, costs, and insurance. At the same time, healthcare is also an economic sector.

In Serbia, the right to personal data protection is enshrined in the Constitution. It mandates that the collection, storage, processing, and use of personal data must be regulated by law. Using such data beyond its original purpose—except for criminal proceedings or national security purposes, as allowed by law—is prohibited. As part of Serbia's EU accession process and its need to harmonize with EU law, the country adopted a new Law on Personal Data Protection in late 2018, with a nine-month delay in implementation.

Unfortunately, as more personal data is left in digital form, instances of misuse are also rising. E-health allows patient data to be exchanged between health and non-healthcare institutions, professionals, and information networks. Whether the harm caused by data misuse is direct or indirect, the patient bears the consequences. A high-quality, well-organized, and efficient healthcare system that embraces innovations like digitization benefits both individuals and society. However, as healthcare digitization grows, so do the risks of abuse—especially concerning sensitive patient data.

This paper emphasizes the importance of personal data protection in an age of digitization and globalization and addresses the potential consequences of patient data breaches.

Importance of the Concept of Privacy in Health Care

Privacy is considered a human right. It is often defined as personal data and information through which individuals allow others access to themselves. Privacy in health care is particularly important for patients and can be

compromised by technologies that monitor people's health and well-being. The right to patient privacy stems from the broader right to privacy, which includes the protection of personal data and serves as an additional guarantee of the inviolability of human integrity. In the local language, "privacy" denotes the personal, intimate, and family sphere of life. In its broadest sense, the right to privacy includes the right of an individual to determine what information about them can be disclosed to others, as well as how their personal data is collected and for what purposes it is used.

Confidentiality is the process of keeping private information secure. This is critical in medical practice, as individuals may avoid seeking care or sharing sensitive information if they cannot trust that their data will remain confidential. A breach of confidentiality—whether due to a security lapse or another reason—undermines trust and raises the risk of data being misused. Data security relies on technical, physical, and administrative safeguards that protect personal information held by an entity. Therefore, privacy, confidentiality, and data security are all essential concepts in modern healthcare. Privacy means the obligation to ensure the confidentiality of personal (health) data, where confidentiality is a person's right to prevent the disclosure of sensitive information to third parties. Confidentiality forms the foundation of the doctor-patient relationship. This view, endorsed by modern legal frameworks, contrasts with earlier paternalistic approaches where doctors made decisions without involving patients. In contrast, contemporary healthcare views confidentiality as a prerequisite for high-quality care. Ensuring the confidentiality of patient health data is both a legal obligation of the healthcare provider and a legal right of the patient. The shift to digital health records has caused a paradigm shift in the healthcare industry. The volume, complexity, and diversity of electronic clinical data are increasing rapidly, contributing to the emergence of "big data."

Driven by the need to improve care, save lives, and reduce costs, electronic health data supports a wide array of critical functions such

as clinical decision-making, health insurance management, disease surveillance, population health monitoring, adverse event tracking, and optimizing treatment for complex diseases. Health data deserves special protection because it often contains highly sensitive and personal information. The public disclosure of such data can cause emotional distress and indirect harm, depending on how others react to that information. Health data is considered a professional secret, and its disclosure may lead to disciplinary, administrative, civil, or even criminal liability. This means that patient medical data—especially if it is accessible to multiple individuals—cannot be publicly disclosed without the consent of the patient or as permitted by law.

To understand privacy protection and the legal responsibilities of healthcare institutions, we must consider what constitutes medical data protected by privacy rights. According to both European and Serbian legal frameworks, "health data" includes personal data related to an individual's physical or mental health, including the provision of health services that reveal information about their health status. Following the WHO definition of health—as a state of complete physical, mental, and social well-being—social conditions may also qualify as health-related data in certain cases. To protect the personal data of its citizens, Serbia enacted the Law on Personal Data Protection, effective from August 21, 2019. The law regulates the use and processing of citizens' personal data, including health information. Its goal is to give individuals the right to privacy and related freedoms, especially regarding the use of sensitive data, including medical records. However, the increasing use of ICT and the Internet has further complicated the issue of privacy protection. For example, if a healthcare worker discloses patient data in another country, they remain legally responsible.

ICT in healthcare offers many advantages. It enables:

1. Access to health information for clinical decision-making, clinical guidelines, and professional literature;
2. Data use for planning, monitoring, and evaluating health services and resources;

3. Support for care planning for individuals, special groups, and populations;
4. Data use in public health research; Evidence-based insights into health status and determinants;
5. Easier fulfillment of international reporting obligations.

Direct Harms of Privacy Breaches

The economic literature on privacy typically focuses on indirect or secondary harms resulting from information flows, which may or may not be influenced by market forces. Within the domain of health privacy, the most closely scrutinized areas are the labor and insurance markets. These are the domains where the misuse of health information can be particularly damaging to individuals and where individuals express the highest concern about potential data disclosures. For example, the disclosure of personal information related to physical or behavioral health conditions can render a worker less attractive to employers. This can negatively impact their employment prospects, compensation, promotion opportunities, and even lead to termination. Discrimination based on health status is often related to, though distinct from, discrimination based on disability. Not all sensitive health information pertains to a disability. Regardless of the motivation behind it, employees who fear negative employer reactions to their health data will prefer to keep such information private.

Insurance markets—including health, life, disability, and long-term care—are another key area where health data plays a role in determining risk profiles. In these markets, it is assumed that health information is used for predictive purposes rather than for overt discrimination. Although privacy risks exist with all forms of medical record-keeping, they are significantly greater for digital records than for paper-based ones. Digital records are easier and cheaper to store, access, and transmit. However, this increased portability can compromise confidentiality and security, exposing data to breaches or misuse by remote attackers. Additionally, digital health data can easily be merged with other datasets, analyzed, and potentially misused, amplifying the risk of

indirect harm. If the right to privacy includes an individual's control over what information is shared and with whom, then stronger privacy protections must be implemented. These protections should aim to limit the scope, flow, and use of digital health data, even if doing so reduces the availability of such data for commercial use.

The Health Care System and Digitization

The healthcare system is one of the most complex components of any country's infrastructure. Each country is responsible for safeguarding the health of its population through accessible and high-quality healthcare services. This includes physical, geographical, and economic accessibility, as well as sustainable financing, healthcare workforce development, and the prioritization of the citizen within the system. The goal of the healthcare system is to preserve and improve public health by providing services through both modern and traditional medicine, in a manner that is effective, affordable, and acceptable to all. Given its significant economic and social role, states implement various policies to ensure stable financing and rational resource management in healthcare delivery.

Modern technological infrastructure—such as internet access, smartphones with embedded sensors, and mobile applications—is now widely accessible. These technologies enable the collection of large volumes of user-contextual data, which can be utilized to enhance healthcare services. One key area benefiting from this is healthcare digitization, where concepts such as e-health and m-health are increasingly implemented.

Advancements in IT and data processing have drastically reduced the cost of data collection and analysis, enabling a transition to digital medical records. Benefits include improved emergency services, reduced patient readmission, and avoidance of redundant testing. Moreover, digital records facilitate compliance with legal and regulatory requirements, support government insurance programs, and aid public health surveillance and disease control. Digital health data also

play a vital role in medical research, enabling large-scale studies, especially on rare diseases and individualized treatment strategies (personalized medicine). Technologies such as AI and machine learning further improve system efficiency and patient care. A study of over 15,000 mobile health apps found that 88% of them include code capable of collecting user data, with most sending data to external entities for tracking, analytics, or advertising.

Data Security in Healthcare

The digitization of healthcare services impacts patients, providers, and the scientific community, with future significance expected to grow. Information systems in healthcare institutions support daily operations, patient record-keeping, and medical data management in both public and private sectors. Developing a robust personal data protection methodology involves:

1. Identifying IT resources that require protection;
2. Describing the system architecture;
3. Identifying and ranking potential hazards;
4. Proposing solutions to mitigate risks;
5. Specifying and implementing recommendations.

Security standards and best practices must evolve with technological advances. Healthcare organizations must frequently update their strategies to counteract targeted cyberattacks and data breaches. In the context of big data analytics, ensuring patient privacy is a growing concern. Data privacy policies determine who is authorized to access, use, and process sensitive data. As regulatory requirements tighten, healthcare organizations are increasingly accountable for storing, maintaining, and transferring sensitive data. However, healthcare remains one of the sectors most vulnerable to cyber attacks. Malicious actors can exploit data mining techniques to expose confidential patient information. Therefore, healthcare providers must adopt strong security frameworks to protect critical data assets and comply with legal standards.

Technologies in Use

Several technologies are employed to protect the privacy and security of health data:

Authentication verifies user identity and limits system access to authorized individuals only.

Encryption protects sensitive data throughout its life-cycle, from collection to storage and transmission. It must be user-friendly and compatible with evolving electronic health records.

Data Masking de-identifies personal data to prevent re-identification while maintaining the data analytical value. This reduces the need for additional security layers during data transfers.

Access Control restricts user permissions based on roles and responsibilities. This is often combined with encryption and authentication techniques to ensure secure, granular access to data.

Conclusion

Healthcare organizations today rely on information systems not only to manage day-to-day operations but also to enhance decision-making, research, and innovation. The integration of information and communication technologies increases the healthcare system's efficiency, improves patient access, and brings financial benefits. The Republic of Serbia is actively advancing its digital health infrastructure. With proper privacy measures, e-health can support both healthcare delivery and medical research, ensuring that digitization serves both individual patients and society as a whole.

Conflict of Interest

The authors declare no conflict of interest.

References

1. Bjegović Mikanović V. Fundamentals of management in the health care system, Belgrade. Ministry of Health of the Republic of Serbia, 2011, p. 18.
2. Pravno-informacioni sistem Republike Srbije. Available at: <http://www.pravnoinformacionisistem.rs/SIGlasnikPortal/eli/rep/sgrs/skupstinstina/zakon/2018/87/13/reg> /Last access on 8.08.2024
3. Klein Tatic V. Professional Secrecy of Health Professionals and the Reasons for Its Disclosure. Foreign Legal Life, Institute of Comparative Law, Belgrade, 2014; 3: 225 – 244.
4. Ferguson T. E-Patient Scholars Working Group. E-Patients : How They Can Help Us Heal Healthcare [Internet]. Boston : Society for Participatory Medicine; 2007; [cited 2024 Nov 15].
5. Law on Personal Data Protection. Official Gazette of the Republic of Serbia, No. 87/2018.
6. Government of the Republic of Serbia. Strategy for the Development of the Information Society in the Republic of Serbia until Official Gazette of RS, 2010. Retrieved from www.digitalnaagenda.gov.rs/dokumenti/ (2020).

7. United Nations. Universal Declaration of Human Rights.
<https://www.un.org/en/universal-declaration-human-rights/>. Published (1948).
8. Keller SA, Shipp S, Schroeder A, Does Big Data Change the Privacy Landscape? A Review of the Issues. *Annu Rev Stat Its Appl* 2016; 3 (1):161-80.
9. Marković R. Constitutional Law, Faculty of Law, University of Belgrade, Belgrade, 2018; p. 475.
10. Westin A. Social and Political Dimensions of Privacy, *J Soc Issues* 2003; 59 (2): 433.
11. Alkhatib S. Waycott J. Buchanan G. Bosua R. Privacy and the Internet of Things (IoT) Monitoring Solutions of Older Adults: A Review. *Comput Inf Syst Univ Melb* 2016; 252:8-1;
12. Kaplan B. How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales. *Camb Q Health Ethics* 2016; 25(2):312-29.
13. Stojković-Zlatanović S. Lazarević B. Confidentiality of personal data - implications for the position of employees from the point of view of case law. *J Law Econ* 2017; 4 -6: 706.
14. Charles C. Whelan T. Gafni A. What do we mean by partnership in making decisions about treatment. *Br Med J* 1999; 1 (319): 781.
15. Warren SD, Brandeis LD. The Right to Privacy. *Harv Law Rev* 1890; 5:193-220.
16. Diligensi A, Pralja D, Cerović D. Data Protection Law – GDPR, Institute of Comparative Law, Belgrade, 2018, 217.
17. Petrović D. Social Construction of Interpersonal Media – From Telegraph to Internet. In: Zbornikradova "Internet idruštvo " (eds. Todorović D, Petrović D, Prlja D. Serbian Sociological Society, Faculty of Philosophy in Niš, Institute of Comparative Law, Belgrade, 2014; pp. 3-22.
18. Hitt LM, Tambe P. Health care information technology, work organization, and nursing home performance. *ILR Review* 2016; 69 (4): 834-859.
19. Mechanic D. The functions and limitations of trust in the provision of medical care. *J Health Polit Policy Law* 1998; 23(4): 661-686.
20. Acquisti A, Brandimarte L, Loewenstein, G. Privacy and Human Behavior in the Age of Information. *Science* 2015; 347 (6221): 509-514.
21. Arrow K. The Theory of Discrimination. In: Ashenfelter O, Rees A, eds., *Discrimination in Labor Markets*, Princeton University Press, 1973.
22. Baldwin ML, Johnson WG. A critical review of studies of discrimination against workers with disabilities. In: Rodgers WM (Ed.) *Handbook on the Economics of Discrimination*. Edward Elgar Publishing, 2006.
23. Posner RA. The Economics of Privacy. *AER* 1981;71(2): 405-409.

24. Freedman S, Lin H, Prince J. Information technology and patient health: analyzing outcomes, populations, and mechanisms. *Am J Health Econ* 2018; 4(1): 51-79.
25. Loertscher S, Marx LM. Digital monopolies: Privacy protection or price regulation? *Int J Ind Organ* 2020; 71: 102623.
26. Tangari G, Ikram M, Ijaz K, Kaafar MA, Berkovsky S. Mobile health and privacy: cross sectional study. *BMJ* 2021; 373:n1248.
27. Natarajan K, Prasath B, Kokila P. Smart health care system using internet of things. *JNCET* 2016; 6 (3): 37.
28. Price WN, Cohen IG. Privacy in the age of medical big data. *Nature Medicine* 2019;. 25(1): 37-43.