AI-driven Health Data Governance: The Risks and Challenges of Datafication

Monica TURINICI[1], Ioana PETCU[2] and Corina PARASCHIV[1]
[1]Université Paris Cité, LIRAES, F-75006 Paris
[2]National Institute for Research & Development in Informatics - ICI Bucharest
monica.bouaru@etu.u-paris.fr, ioana.petcu@ici.ro, corina.paraschiv@u-paris.fr

Abstract: Artificial intelligence (AI) integration in healthcare is transforming data governance and profoundly impacting medical practice. While AI promises advancements in diagnostic accuracy and personalized treatments, it also raises major concerns regarding data security, data privacy, fairness, and the autonomy of healthcare professionals. This article examines how the datafication of healthcare, where medical data becomes a valuable and contested resource, generates new ethical issues regarding the access to medical data, patient consent, and data security. Based on a thorough literature review, the article highlights key challenges in the AI-driven medical data governance and identifies potential risks of datafication, such as fragmentation of access, security breaches, patient misinformation, unauthorized medical data use, data commercialization, or the erosion of medical privacy.

Keywords: AI in healthcare, medical data governance, patient consent, medical data privacy, data commercialization, risks of datafication

INTRODUCTION

The European Union (EU) is playing an important role in creating, developing, and strengthening a European Health Union. The main goal is to ensure that all Member States are equipped to deal with health crises, have access to affordable and innovative medical supplies, and collaborate to improve disease prevention, treatment and follow-up.

On 21st January 2025, the EU Parliament and the Council of the EU adopted new measures regarding the Regulation of European Health Data Space (EHDS), a regulatory framework that aims to enhance individuals' digital access to their data, foster a unified market for electronic health records and AI systems, and ensure a secure use of the health data for research and policy-making. EHDS is a key pillar of the European Health Union, building

https://doi.org/10.54851/v7i1y202504

on General Data Protection Regulation (GDPR) and the Network and Information Systems Directive 2 (NIS 2) to strengthen the healthcare collaboration and crisis response across the EU.

The regulation of EHDS targets to improve people's access to and control over their medical data, while also seeking to support the use of the health data for such societal benefits as promoting research, accelerating innovation, increasing preparedness to respond to health crisis, allowing for personalized medicine, promoting patient safety, preventing pandemics, and improving policy-making and regulation. Additionally, it aims to strengthen the internal market by establishing a consistent legal and technical framework for developing, marketing, and using electronic health record systems in line with the EU values (Radu et Petcu, 2021).

The reinforcement of the collection, analysis and exploitation of the health-related data is at the center of the different EU health-related political initiatives. This article examines how the datafication of healthcare, where medical data becomes a valuable and contested resource, generates new challenges and risks. In particular, it studies how the adoption of AI in healthcare (Petcu et al., 2022) is redefining the health data governance. The analysis focuses on the restricted access to patient information, patient consent, and the erosion of medical confidentiality. The main contribution of the research is to highlight the key risks stemming from a health data governance based on AI.

The rest of the paper is organized as follows. After defining the datafication in the health domain and discussing the AI-driven health data governance, it focuses on the risks and challenges of insuring controlled medical data access, patient consent, and data security.

DATAFICATION IN THE HEALTH DOMAIN

Introduced in 2013 by Kenneth Cukier and Victor Mayer-Schonberger, the concept of "datafication" refers to a process by which human, social and biological activities are transformed into electronic data, which can be monitored, tracked, analyzed, and optimized (Mayer-Schönberger et al., 2013). This large-scale transformation of different activities into machine-readable data allows to extract more knowledge and information, promoting data-driven organizations (Van Dijck, 2014). By turning activities into valuable data, the datafication enables companies to optimize processes such as predicting customer preferences, personalizing content, improving risk assessment, or predicting fraud behavior.

Figure 1 provides an example of how datafication in healthcare transforms the medical research by using the AI. It illustrates the technological trend of transforming different aspects of human lives into computerized data processed by AI tools that convert the information contained in these data into new forms of value.

The widespread of the artificial intelligence (AI) and the expansion of data storage and processing capacities have accelerated the datafication trend, raising both opportunities and risks (Floridi and Cowls, 2022). For instance, patient monitoring and medical records produce vast amounts of data, enabling clinical decision-making to deliver more personalized, proactive, and effective care (Ebeling, 2016). Moreover, the use of advanced algorithms and machine learning technologies is significantly improving the diagnostic accuracy (Petcu et al., 2022) and contributes to the development of the customized treatments, tailored to individual patient needs. The easy access to healthcare data further supports the medical research, predictive diagnostics, precision medicine, and the development of innovative AI-powered healthcare tools.

However, the widespread adoption of AI-based solutions in healthcare generates significant challenges related to data security and data privacy (Lascateu and Constantinescu, 2024), while also bringing critical discussions about the informed patient consent. It also raises the question of the role and status of the doctors facing an increasing empowerment of the data systems. According to Ruckenstein et Schull (2017), the datafication can distance the healthcare professionals from their clinical

Figure 1. *Datafication in healthcare transforms medical research using AI*
Source: picture generated using an AI tool

knowledge by transforming them into mere users of algorithmic solutions with a progressive loss of their control over the medical decisions.

The scientific literature dealing with datafication in healthcare explores this issue from different angles, examining its implications for data governance, the transformation of the decision-making processes, and patient monitoring and treatment. In what follows, the focus is on the health data governance.

HEALTH DATA GOVERNANCE

Health data governance refers to the set of rules and mechanisms that regulate the access, use and protection of the health data. The increasing spread of the connected medical devices (IoT), centralized databases and cloud computing systems is driving to a radical transformation in data governance practices (Petcu et al., 2022).

Figure 2 summarizes the main goals of the health data governance in relation to the datafication in the health domain and the development of the AI. The figure highlights the multiplication of the health data that now include not only the medical data from hospital and disease records, the pharmaceutical data, and the biological data from laboratories, but also the behavioral data from the social media data and the health application data.

The fast development of the AI in the health sector triggers innovative opportunities for optimizing the medical services by exploiting the increasing amount of the health data available. The AI tools and applications may contribute to producing new medical knowledge, redefining disease classifications or predicting individual health evolution paths. At the same time, the AI devices used in the patient record management, the early pathology detection, and the treatment recommendation rely on the algorithmic analysis

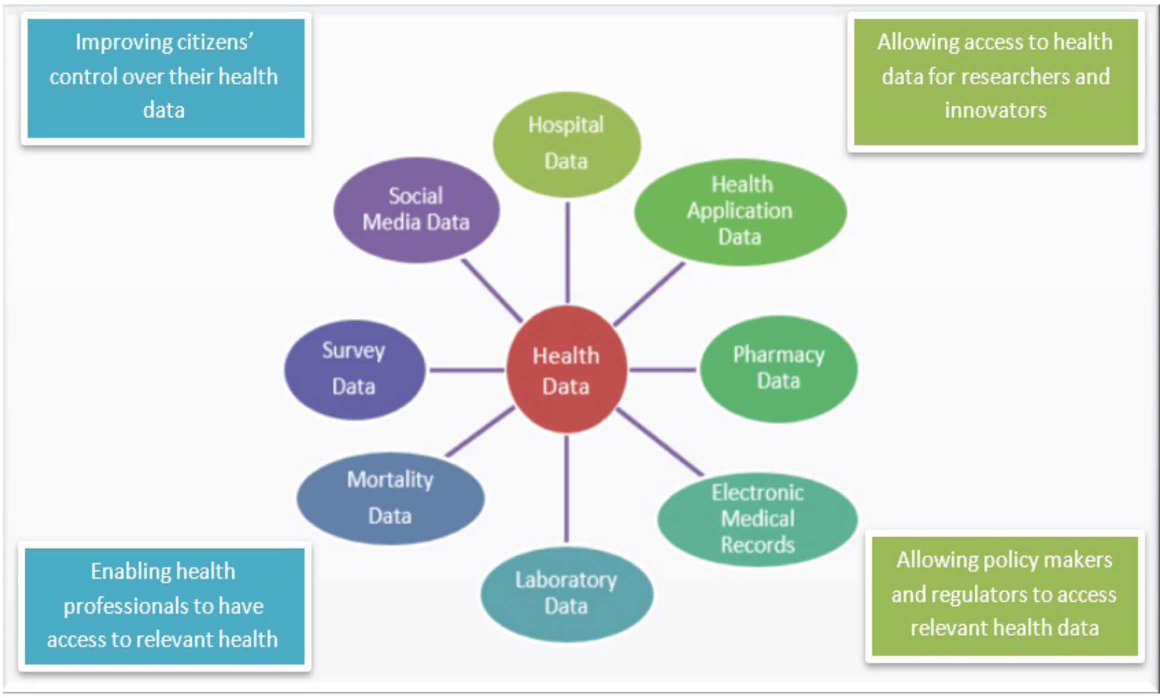

Improving citizens' control over their health data
Allowing access to health data for researchers and innovators
Hospital Data
Social Media Data
Health Application Data
Survey Data
Health Data
Pharmacy Data
Mortality Data
Electronic Medical Records
Laboratory Data
Enabling health professionals to have access to relevant health
Allowing policy makers and regulators to access relevant health data

Figure 2. *Datafication and Health Data Governance*
Source: adapted by the authors

of massive streams of heterogeneous data, which generates major challenges in terms of data privacy, interoperability, and accessibility (Pussewalage and Oleshchuk, 2019). In addition, the fragmentation of the healthcare data, combined with the increasing use of cloud and edge computing environments, exacerbates the vulnerability risks for hospitals and the medical institutions, particularly from cyberattacks and potential gaps in the protection of the healthcare data (Sun et al., 2024). The extensive use of the AI technologies may also impact on the autonomy of the healthcare professionals. Therefore, it is crucial to develop appropriate regulatory frameworks to ensure the ethical and secure implementation of these emerging technologies (Paraschiv et al., 2023).

The first comprehensive legal framework on the AI worldwide is the EU Regulation 2024/1689 on AI. It aims to ensure that the AI systems are developed and used responsibly, addressing AI-related risks such as bias, discrimination and accountability gaps, while promoting innovation and encouraging the adoption of AI. The AI Act Regulation is an important step towards the ethical and responsible use of the AI in the EU. The main rules imposed by the AI Act, which is to be implemented gradually until 2026, relate to the classification of the risks in 4 categories depending on their level– see Figure 3 – based on transparency and accountability, protection of personal data and training of the staff using these technologies. Thus, there can be distinguished minimal risks, limited risks, high risks and unacceptable risks.

The analysis of the literature dealing with health data governance allows us to identify three major challenges from a cyber security perspective that need to be addressed in the datafication process. These challenges include the medical data access, patient consent, and medical data security. These three challenges with their associated risks will be discussed in detail in the following sections.

MEDICAL DATA ACCESS

The access to the healthcare data by the professionals, researchers, and private compagnies is an emerging and complex

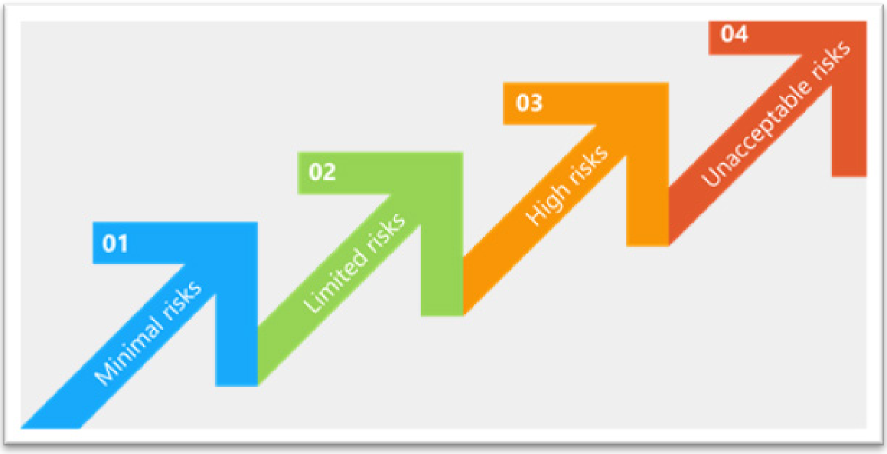


Figure 3. *Classification of risks depending on risk level*
Source: adapted by the authors

issue, requiring a balance between making the information available to the adequate actors at the right moment for the optimal patient care and protecting the confidentiality of the medical data. Excessive restrictions on data access may hamper the medical staff's ability to provide quality care, while an overly broad access can increase the risk of confidentiality breaches (Greenhalgh et al., 2018). As an illustration, the opening of the healthcare data for research in France has given rise to a lot of debate and controversy, in particular regarding the increase in the likelihood of data misuse, unauthorized handling, and non-ethical exploitations (Fallery, 2021). Analyzing the challenges associated with the access to the health data for researchers and professionals, different authors highlight the need to reconcile data openness to foster research and innovation, while ensuring the protection of the patient privacy (Winter and Davidson, 2022). The literature converges on the need to strike the right balance between a wider access to healthcare data, essential for effective patient care, and the implementation of the protection mechanisms to safeguard the confidentiality and the ethical use of this sensitive information. A wider access to data can not only allow to exploit these data to generate new knowledge and to support strategic and operational decision-making, but also to enable the citizens to better control the administration (Fallery, 2021).

Table 1 summarizes the main challenges and risks of datafication with respect to the medical data access. These risks include those regarding data sovereignty, limited access to the medical patient history, fragmentation of the access rights, the commercial use of the data or biased scientific research. The table highlights, for instance, the risk of a growing asymmetry in the access rights between those who produce the data (medical staff) and those who manage it (IT departments, storage companies, AI platforms). The tendency is to shift control over the decisions regarding the medical data access from doctors towards IT actors. However, non-medical personnel do not always understand the medical care processes and the type of access rights that are adequate for optimal patient care.

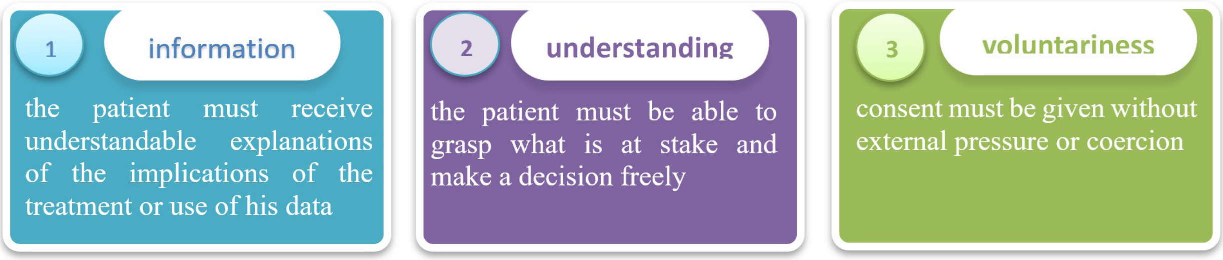
Another important aspect includes the risk of a shift towards a commercial use of medical data, to the detriment of the general interest and medical confidentiality. With medical data becoming a commodity like any other, we also face a higher risk of illicit data trading, leading to a potential exploitation of patient information. These risks are increased by the emergence of the digital platforms where the patients themselves submit their data, often under the impetus of private actors.

Table 1. *Challenges and risks regarding medical data access*

Major Challenges	Generated Risks
Medical data sovereignty	Risk of non-medical personnel having access to medical data Loss of sovereignty of the medical staff on decisions regarding health data access Risk of the medical staff having limited access to the patient medical history based on decisions by administrators and the IT personnel
The fragmentation of access rights	Risk of a fragmentation of access rights leading to inconsistencies in the care pathway Risk of differentiated access rights depending on location and entity Risk of differentiated access management depending on the profile of the user
Biased scientific medical research	Risk of prioritizing publication metrics over patient welfare in medical research Ethical concerns related to the access to patient data for research Risk of compromising the integrity in medical research through increased AI-use
Commercialization of sensitive data	Risk of a commercial logic in which medical data become a commodity Risk of illicit data trading Risk of data misuse and unauthorized handling

PATIENT CONSENT

The regulatory framework regarding datafication in the health domain imposes informed consent protocols. However, numerous studies (Dove and Taylor, 2021; Vikas et al., 2021; Hurley et al., 2025) show that patients often sign these forms without fully grasping their implications. The informed consent is a fundamental principle of the bioethics and the medical law. It rests on three essential pillars: information, understanding, voluntariness (Sherman et al., 2021). Information refers to the moral duty of the medical staff and health companies to provide adequate and complete explanations to the patients about the short- and long-term implications of the treatments, as well as the type and the extent of use of their personal data (Resnik and Pugh, 2024). Understanding refers to the capacity of the patient to understand the message received, in particular the comprehension of the critical information, including the technical information (Hurley et al., 2025). Voluntariness refers to the absence of any external pressure or manipulation, allowing the patient to make decisions freely (Sherman et al., 2021). Figure 4 provides a synthetic view of these three pillars of informed consent.


1 information

the patient must receive understandable explanations of the implications of the treatment or use of his data

2 understanding

the patient must be able to grasp what is at stake and make a decision freely

3 voluntariness

consent must be given without external pressure or coercion

Figure 4. *Essential pillars of informed consent*
Source: adapted by the authors

Datafication and the introduction of AI in healthcare has the potential of making the dynamics of obtaining patient consent more complex (Floridi and Cowls, 2022). Indeed, empirical studies show that patients do not clearly perceive the secondary use of their data by the AI systems and do not realize the implications of the algorithmic sharing of the medical information (Sharon, 2021). This lack of understanding raises concerns about health data governance and the social acceptability of the AI in the medical sector (Mittelstadt, 2019). Moreover, ethicality is under question because the way consent forms are presented does not provide an alternative solution to the patients in need for a medical treatment, imposing them to give their consent.

Consent is also closely linked to patients' perception of risk and trust. According to Grote and Berens (2020), several factors influence the acceptability and governance of the medical data sharing. First, there is the "black-box problem", as the AI algorithms are often perceived as opaque and incomprehensible, limiting patient trust (Rudin and Radin, 2019). Regarding this point, the literature shows that consent is not possible if the length, the terminology or the content of the consent form is not adequate (Hurley et al., 2025), which is often the case when the AI systems are used. Second, there is the risk of the health data misuse. Indeed, medical marketing studies show that patients fear that their information will be used for commercial purposes or shared with other actors without their explicit consent (Sharon, 2021). Third, there is the risk of the algorithmic error, as an AI-generated misdiagnosis can be perceived as a threat, especially if the patient doesn't understand how the algorithm works (Gerke et al., 2021). The stakes are high because without a truly informed consent, the digital transformation of the medical sector could weaken the patient-caregiver relationship and generate increased mistrust regarding new healthcare technologies.

Table 2 provides a summary of the different challenges and risks associated to patient consent. It highlights the current ambiguity in consent, as well as the risk of a lack of patient awareness about the actual use of their data, which is likely to increase with AI use.

Table 2. *Challenges and risks regarding patient consent*

Major Challenges	Generated Risks
Purpose of Consent regarding AI	Risk of patient manipulation by exposing only the benefits of consent without full information about the risks of data sharing and AI use Risk of patients agreeing unknowingly to terms that compromise their privacy Risk of ambiguity of consent, often vague regarding AI
Medical ethics regarding consent	Risk of violation of ethical and legal principles regarding consent Risk of medical data being repurposed after consent without patient awareness Risk of patients' data being used by AI for purposes beyond their knowledge or approval.
Traceability of medical information after consent	Risk of fraud as medical data, once shared, may be difficult to track Risk of uncontrolled circulation of data between departments and hospitals and sometimes internationally, without the patient being informed Risk of patient being unable to retract consent once data shared
Patient autonomy in decision-making	Risk of AI use increasing medical paternalism Risk of loss of patient autonomy in decision-making Risk of limiting patient control over who and when has access to their own medical information

Indeed, if the patients are only exposed to the benefits of data sharing without full information about the risks and future use of the data, the consent obtained might be perceived as manipulated. First, patients may unknowingly agree to terms that compromise their privacy or data security. Second, ethical dilemmas may arise when patient data are used for purposes beyond their knowledge or approval. These types of problems generally occur after patient consent, when the data circulate between departments, between hospitals, and sometimes even internationally, without the patient being informed. Data that should be secret and the patient's property might then be abused, generating a risk of possible drift towards a medicine of surveillance and control.

MEDICAL DATA SECURITY

Digitization and inter-institutional data sharing increase the risk of leaks and breaches of medical confidentiality (Kiener, 2021). The management literature highlights the tensions between the benefits of data centralization and the risks of loss of control for the healthcare professionals. This issue is also addressed in the context of the privacy paradox (Paraschiv and Ayadi, 2024), according to which individuals express concerns about data protection while adopting behaviors that favor their exposure. Table 3 offers an analysis of the main risks and challenges of datafication in relation to data security.

The massive collection and exploitation of healthcare data, notably via technologies

Table 3. *Challenges and risks regarding data security*

Major Challenges	Generated Risks
Data leaks and vulnerabilities	Risk of large-scale cyberattacks and data leaks Risk of AI health-platforms introducing biases, errors, or vulnerabilities in data security. Risk of data duplication increasing the risk of inefficiencies, miscommunication, and delayed treatments Risk of medical care decisions being taken by algorithms without consultation with healthcare professionals.
Biased use of AI algorithms	Risk of biases in algorithmic decision-making Risk of incorrect use of algorithms producing unfair or prejudiced outcomes due to issues with the data or biased algorithms Risk of lack of transparency about algorithmic results
Interconnectivity of health databases	Risk of erosion of medical privacy with the increase in the number of stakeholders accessing medical data Risk of open medical databases, accessible to more people, from medical staff to administrators and to IT engineers. Risk of unauthorized access leading to patient privacy violations
Lack of medical confidentiality	Risk of breaches in confidentiality Risk of erosion of patient trust Risk of compromising the doctor-patient relationship Risk of loss of control over medical privacy
Exploitation of medical data in other domains	Risk of monetization of medical data without consent Risk of health data unauthorized exploitation leading to privacy violations Risk of private stakeholders from the pharmaceutical sector increasingly using data from hospitals and laboratories without consent. Risk of patients' medical information being used by insurance companies.

such as smart sensors and virtual medical assistants, raises issues of data security and anonymization (Cerruto et al., 2022). The reliance on the cloud infrastructures for data storage and exchange between patients and the healthcare professionals exacerbates the risks of sensitive information leakage and non-compliance with the current regulations, such as the GDPR in EU. Indeed, several studies show that the medical AI platforms do not always guarantee a clear traceability of data use or sufficient transparency on how algorithms work (Rudin and Radin, 2019). The „black-box AI" phenomenon, where medical decisions are influenced by opaque and difficult-to-interpret algorithms, accentuates the feeling of vulnerability of the medical staff, who may find themselves unable to justify AI-driven clinical decisions to their patients or the health authorities (Kiener, 2021; Beltramin, 2022; Wadden, 2022).

CONCLUSION

This article highlights key points that make an innovative contribution to the understanding of the issues related to the AI and health data governance. While most studies on the AI-driven health applications focus on benefits in terms of optimizing care, reducing medical errors, or improving diagnosis (Esteva et al., 2019), this article analyses the new challenges and risks raised by the datafication process in the medical sector.

The study points to the transformation of the medical data, under the influence of the AI, into an economic resource exploited by private companies (Grote and Berens, 2020). Contrasting to the work that focuses on the protection of the patient data under the personal data protection regulation or other regulations (Pussewalage and Oleshchuk, 2019), this approach explores how the patients and the medical staff become producers of data whose use they no longer control, especially when facing the pharmaceutical industries and the medical big data players. This loss of sovereignty over the health information has rarely been addressed from this angle (Radu et al., 2022).

Finally, this perspective is not limited to a simple reflection on the cyber risks associated with the management of the health data. To better understand the structural tensions between the technological innovation and the preservation of the fundamental values of the health care, the present point of view crosses several disciplinary fields, including the ethics in medicine (patient confidentiality, consent, decisional autonomy), the management of the health care organizations (IT services, cloud data regulation), and the economics of the health care (the commodification of data, the financial stakes of big data in health).

ACKNOWLEDGEMENT

This research received support from the French government under the France 2030 investment plan, as part of the Initiative d'Excellence d'Aix-Marseille Université – AMIDEX AMX-22-RE-AB-003.

REFERENCE LIST

Beltramin, D., Lamas, E. & Bousquet, C. (2022) Ethical issues in the utilization of black boxes for artificial intelligence in medicine. *In Advances in Informatics, Management and Technology in Healthcare*, IOS Press, 249-252.

Cerruto, F., Cirillo, S., Desiato, D., Gambardella, S. M. & Polese, G. (2022) Social network data analysis to highlight privacy threats in sharing data. *Journal of Big Data*, 9(19), 1-26.

Dove, E. S. & Taylor, M. J. (2021) Signaling standards for progress: bridging the divide between a valid consent to use patient data under data protection law and the common law duty of confidentiality. *Medical Law Review*, 29(3), 411-445.

Ebeling, M.F.E. (2016) Healthcare and big data: digital specters and phantom objects, *New York: Palgrave Macmillan*.

Fallery, B. (2021) La plateforme de données de santé Health data hub. *Revue Française de Gestion*, 297(4), 141-159.

Floridi, L. & Cowls, J. (2022) A Unified Framework of Five Principles for AI in Society. In: Carta, S. (Ed.), Machine *Learning and the City: Applications in Architecture and Urban Design*, John Wiley & Sons Ltd., Hoboken, 535-545.

Gerke, S., Minssen, T. & Cohen, G. (2021) Ethical and Legal Challenges of Artificial Intelligence-Driven Healthcare (2020). In Bohr, A., Memarzadeh, K. (eds.), *Artificial Intelligence in Healthcare, 1st edition, Elsevier*. 295-336.

Greenhalgh, J., Dalkin S. & Gibbons E. (2018). How do aggregated patient-reported outcome measures data stimulate health care improvement? A realist synthesis. *Journal of Health Services Research & Policy*, 23(1), 57-65.

Grote, T. & Berens, P. (2020) On the ethics of algorithmic decision-making in healthcare. *Journal of Medical Ethics*, 46(3), 205-211.

Hurley, M. E., Lang, B. H., Kostick-Quenet, K. M., Smith, J. N. & Blumenthal-Barby, J. (2025) Patient consent and the right to notice and explanation of AI systems used in health care. *The American Journal of Bioethics*, 25(3), 102-114.

Kiener, M. (2021) Artificial intelligence in medicine and the disclosure of risks. *AI & society*, 36(3), 705-713.

Lascateu, C. & Constantinescu, M. (2024) Bridging the Maturity Gap: Adaptive Strategies for Advancing Cybersecurity in Romanian Healthcare Institutions, *Romanian Cyber Security Journal*, ISSN 2668-6430, 6(2), 3-13, doi: 10.54851/v6i2y202401

Mayer-Schoenberger, V. & Cukier, K. (2013) Big Data. A Revolution that will transform how we live, work, and think. *London: John Murray Publishers*.

Mittelstadt, B. (2019) Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1(11), 501-507.

Paraschiv, C. & Ayadi, N. (2024) Ethicality of online dynamic pricing: an empirical investigation of consumer perception of ethical risks. *Journal of Revenue Pricing and Management.* doi: 10.1057/s41272-024-00497-3

Paraschiv, C., Ayadi, N., Rousset, X. & Turimici, M. (2023) Consumer Vulnerability to dynamic pricing in online anvironments. *Applied Economics*, 56(25), 3032-3047.

Petcu, I., Barbu, D.C., Negoita, S.I. (2022) Techniques based on intelligent algorithms used in skin cancer prevention - *Romanian Journal of Information Technology and Automatic Control*, Vol. 33, Nr. 2

Pussewalage, H. S. G. & Oleshchuk, V. A. (2019). An anonymous delegatable attribute-based credential scheme for a collaborative e-health environment. *ACM Transactions on Internet Technology*, 19(3), 1-22.

Radu, A. F., Petcu, I. & Barbu, D.C. (2022) Privacy and security – related challenges of the future EU Digital Identity" – *Romanian Cyber Security Journal*, 4(2).

Radu, A. F. & Petcu, I. (2021) Intrinsic aspects of e-Government consolidation across the European Union. Case study: Romania. *Romanian Journal of Information Technology and Automatic Control*. 31(4), 83-96. doi: 10.33436/v31i4y202107.

Resnik, D. B., & Pugh, J. (2024) Green bioethics, patient autonomy and informed consent in healthcare. *Journal of Medical Ethics*, 50(7), 489-493.

Ruckenstein, M., Schüll & N. D. (2017). The Datafication of Health, *Annual Review of Anthropology*, 46(1), 261-278, doi: 10.1146/annurev-anthro-102116-041244

Rudin, C. & Radin, J. (2019) Why are we using black box models in AI when we don't need to? A lesson from an explainable AI competition. *Harvard Data Science Review*, 1(2), 1-9.

Sharon, T. (2021) Blind-sided by privacy? Digital contact tracing, the Apple/ Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*, 23(Suppl 1), 45-57.

Sherman, K. A., Kilby, C. J., Pehlivan, M. & Smith, B. (2021). Adequacy of measures of informed consent in medical practice: a systematic review. *PLOS One*, 16(5), e0251485.

Van Dijck, J. (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & society*, 12(2), 197-208.

Vikas, H., Kini, A., Sharma, N., Gowda, N. R., Gupta, A. (2021). How informed is the informed consent? *Journal of Family Medicine and Primary Care*, 10(6), 2299-2303.

Wadden, J. J. (2022). Defining the undefinable: the black box problem in healthcare artificial intelligence. *Journal of Medical Ethics*, 48(10), 764-768.

Winter, J. S., Davidson, E. (2022). Harmonizing regulatory regimes for the governance of patient-generated health data. *Telecommunications Policy*, 46(5), 102285.