MEDWIN PUBLISHERS
Committed to Create Value for Researchers

Annals of Bioethics & Clinical Applications
ISSN: 2691-5774

Artificial Intelligence in Healthcare: Bioethical and Legal Challenges in the Brazilian Context

Madeira CSP*

National Cancer Institute, Ministry of Health, Brazil

***Corresponding author:** Christiane Soares Pereira Madeira, National Cancer Institute, Brazil, Tel: 55 21 991124145; Email: christiane.pereira@inca.gov.br

Mini Review

Volume 9 Issue 1

Received Date: January 14, 2026

Published Date: January 29, 2026

DOI: 10.23880/abca-16000284

Abstract

Artificial Intelligence (AI) has rapidly developed, expanding from basic machine reasoning in the 1950s to modern techniques like machine learning and generative AI. These advancements have enabled important healthcare applications such as diagnostic imaging, telemedicine, patient monitoring, and drug discovery. Despite improved efficiency and accuracy, AI introduces ethical and legal concerns including data privacy, informed consent, fairness, liability, and cybersecurity. Effective regulation is needed to address these challenges and support responsible use of AI in healthcare.

Keywords: Artificial Intelligence; Healthcare; Bioethics; Cybersecurity

Abbreviations

AI: Artificial Intelligence; EBIA: The Brazilian Strategy for Artificial Intelligence; MCTI: Ministry of Science, Technology and Innovation; HIPAA: Health Insurance Portability and Accountability Act; MSKCC: Memorial Sloan Kettering Cancer Center; MDR: European Medical Device Regulation; GDPR: General Data Protection Regulation; ANPD: National Data Protection Authority; LGPD: General Data Protection Law; IP: Intellectual Property

Introduction

Artificial Intelligence (AI) did not emerge at the turn of the millennium. Its trajectory dates back to the 1950s, when the first studies on machines capable of "thinking" appeared. Since then, the field has progressed into machine learning and deep learning, which have significantly contributed to contemporary advancements. AI is commonly divided into broad categories such as weak AI, focused on specific tasks, and strong or superintelligent AI (a hypothetical form with human level cognitive capacity), as well as generative AI, capable of creating text, images, and complex analyses. There is also a technical subdivision that includes machine learning, deep learning, computer vision, natural language processing, expert systems, and intelligent robotics [1].

In the healthcare sector, these technologies, when integrated with artificial intelligence have become essential, supporting everything from intelligent patient screening and telemedicine, already a reality in Brazilian hospitals to advanced diagnostic imaging, continuous monitoring through wearable devices, and the prediction of diseases before symptoms appear, as well as accelerating the discovery of new therapeutic drugs [2].

The application of AI in healthcare represents a global innovation, particularly in medical diagnosis, driven by improvements in diagnostic imaging and the optimization of hospital processes and workflows, which make patient care

more efficient. However, this technological advancement also raises important ethical and legal challenges in the field of bioethics, including issues such as informed consent, the protection and privacy of sensitive data, transparency, algorithmic fairness, and potential biases [3].

From a legal perspective, key concerns include safety and effectiveness in the use of AI, the allocation of responsibility in cases of medical error, cybersecurity, and intellectual property. These issues are widely discussed in the United States, Europe, and Brazil [4].

This article aims to examine the concepts of artificial intelligence and explore the bioethical and legal challenges associated with its application in healthcare within the Brazilian context.

AI concepts in Brazil

Our analysis begins from a bioethical and legal perspective, grounded in the definition of artificial intelligence adopted within the Brazilian context. According to Associação Brasileira de Normas Técnicas (ABNT NBR ISO/IEC 22989:2023) [5], an artificial intelligence system is defined as:

"*...a computer-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or make decisions that influence real or virtual environments*."

The Regulatory Framework for Artificial Intelligence (PL 2.338/2023 and its substitutes) [6], approved by the Federal Senate presents the following official definition:

"*... a machine-based system that, with different degrees of autonomy and for explicit or implicit purposes, infers, from a set of data or information it receives, how to generate results, in particular prediction, content, recommendation or decision that may influence the virtual, physical or real environment*."

The Brazilian Strategy for Artificial Intelligence (EBIA) [7], issued by the Ministry of Science, Technology and Innovation (MCTI), adopts the Organization for Economic Co-operation and Development's definition of artificial intelligence:

"*AI is best understood as a set of techniques designed to emulate some aspects of the cognition of living things using machines. [...] An AI system is a machine-based system that can, for a given set of human-defined goals, make predictions, recommendations, or decisions that influence real or virtual environments. AI systems are designed to operate with varying levels of autonomy.*"

This conceptual analysis concludes by presenting the adopted in the Brazilian Plan for Artificial Intelligence (PBIA – 2025–2028) [8], coordinated by the MCTI, which defines AI for public policy purposes as:

"*A set of models, algorithms, techniques, and methodologies that can be implemented as computational systems that produce results such as predictions, classifications, recommendations, and decisions, based on learning processes based on large volumes of data, with the potential to influence physical and virtual environments*."

The different definitions of AI in the Brazilian context reveal important nuances in its technical, legal, and political framing. The ABNT standard emphasizes the computational nature of AI and its dependence on human-defined objectives, reinforcing the centrality of human supervision. The Regulatory Framework, in contrast, broadens the concept by acknowledging degrees of autonomy and implicit objectives, recognizing the complexity of contemporary systems. EBIA, aligned with the OECD, characterizes AI as a set of techniques that emulate aspects of cognition, with an emphasis on varying levels of autonomy. Finally, the PBIA adopts a pragmatic, policy-oriented perspective, highlighting the role of large-scale data and learning processes. Taken together, these definitions illustrate the ongoing tension between human control, algorithmic autonomy, and the social impact of AI [5-8].

In Brazil, regardless of the AI concept adopted, several public sectors such as health, education, security, and culture have published specific national guidelines for its use, consistently aligned with ethical principles, data protection, transparency, and human oversight. In the case of the Ministry of Health, the use of AI is directed toward decision support, anomaly detection, and diagnostic optimization, always accompanied by impact assessments and measures to mitigate risks to human health [9].

Bioethical and Legal Challenges of the Use of AI in Healthcare

The advent of AI in Brazil presents an opportunity for significant advances in Digital Health, expanding access to healthcare and education in a country of continental dimensions. Consequently, bioethical challenges become essential points of reflection for society as a whole. Among the main challenges are informed consent, issues related to information security and transparency, the need for algorithmic fairness and bias control, and the protection of data privacy [9].

The deployment of AI in the medical field substantially transforms the interaction between doctors and patients,

prompting discussions about the appropriate procedures for obtaining informed consent regarding the use of these advanced technologies. The level of detail required for professionals to explain to patients how AI systems function, what types of data they use, and the potential biases inherent in these systems is not yet clearly defined. This challenge becomes even more pronounced in the case of "black box" algorithms those whose internal decision-making processes are unknown or cannot be explained. In such cases, not even developers are able to fully describe how the AI reaches its conclusions [10].

In addition, ensuring information security is essential, as is training AI systems with reliable and properly validated datasets. Developed in partnership with the Memorial Sloan Kettering Cancer Center (MSKCC), Watson for Oncology was presented as a tool capable of analyzing medical records and scientific literature to recommend personalized cancer treatments. The case has since become a classic example of failure in the application of AI to healthcare, frequently cited in academic studies and public policy reports. It is important to emphasize that experiences such as the IBM Watson for Oncology case where inadequate recommendations resulted from the use of synthetic cases rather than authentic clinical data serve as critical reminders of the need for caution when adopting new AI systems in health. Transparent disclosure of a system's functioning and limitations is fundamental to building trust among healthcare professionals and patients [11].

It is essential to remember that AI systems are created by humans, which makes it necessary to ensure algorithmic fairness and control potential biases, since there is a risk that these systems may perpetuate discrimination based on ethnic origin, gender, age, or special needs [10]. This discussion extends beyond the medical sphere and enters the legal domain, requiring the development and application of new legislation to determine responsibilities and provide remedies for potential harms [1].

The vast amount of health information collected through Big Data raises concerns about data ownership and the methods used to safeguard it. When such information is misused, it can lead to negative consequences for patients, including restrictions on access to insurance, impacts on professional opportunities, and even repercussions in their personal relationships. For this reason, the privacy of sensitive data must remain a central topic of debate in the use of AI in the medical field and related areas [1,10].

The trajectory of our discussion makes it clear that the use of AI will soon confront us with significant legal challenges, and that in the near future, if not already, we must be prepared for litigation involving AI systems in healthcare. In the United States and Europe, artificial intelligence is regulated within the framework of medical device legislation to ensure its safety and effectiveness. A persistent challenge, however, is adapting regulatory frameworks such as the European Medical Device Regulation (MDR) to appropriately classify machine-learning-based software and to guarantee that such systems continue to meet safety standards as they evolve [2,4].

The determination of civil liability for medical errors arising from the use or support of artificial intelligence systems is considerably complex. At present, it is accepted that the physician remains the central figure of accountability, even when relying on opaque ("black box") algorithms with limited auditability. Some studies propose the adoption of strict liability for manufacturers or the creation of specific compensation funds to address potential harms [12].

When the discussion turns to data protection and privacy, significant legal gaps become evident. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) a federal law enacted in 1996 to safeguard the privacy and security of patients' health information does not extend its protections to health data generated by applications outside the scope of traditional healthcare entities, such as those developed by major technology companies [13]. In Europe, the General Data Protection Regulation (GDPR), the landmark legislation that came into force on May 25, 2018, and has become a global reference in privacy and personal data protection offers more comprehensive safeguards. Nevertheless, debates continue regarding the extent of patients' "right to explanation" in automated decision-making processes [14].

Across the world, despite the existence of data-protection laws, computerized health systems continue to present vulnerabilities some minor, others significant, that can be exploited by cyberattacks. Such breaches place the privacy and security of patient data at risk and may even allow the manipulation of algorithms, potentially leading to incorrect diagnoses. A concrete example of this fragility was the "WannaCry" ransomware attack, one of the largest cyber incidents in history. Occurring on May 12, 2017, it infected more than 200,000 computers in over 150 countries. The attack exploited a Windows vulnerability known as EternalBlue, encrypted victims' files, and demanded payment in Bitcoin to restore access. This episode demonstrated how outdated operating systems and unresolved security flaws can trigger global crises, underscoring the critical importance of regular updates, robust backup practices, and comprehensive cybersecurity strategies [15].

The Brazilian legal frameworks governing data protection and the use of artificial intelligence form a complementary

ecosystem aimed at balancing innovation, fundamental rights, and transparency. The General Data Protection Law (LGPD) serves as the central pillar, establishing principles and limits for any automated processing of personal data, while the Civil Rights Framework for the Internet reinforces guarantees of privacy and accountability in the digital environment. The Access to Information Law adds an essential layer for the use of AI by public authorities, requiring transparency regarding algorithms that affect citizens' lives. PL 2.338/2023, currently under discussion in Congress, proposes a specific regulatory framework for AI, aligned with the LGPD and guided by a risk-based approach, defining obligations for developers and operators. The role of the National Data Protection Authority (ANPD), through technical notes and guidelines, integrates these instruments by interpreting the LGPD in AI-related contexts and guiding the development of coherent and protective regulation [16].

The debate over Intellectual Property (IP) highlights a growing tension between the commercial protection of artificial intelligence through patents and trade secrets and the broader societal need for open science and data sharing. While companies argue that strong IP rights are essential to safeguard investments and incentivize innovation, researchers emphasize that open access to data and algorithms accelerates scientific progress, particularly in fields like health care where collaboration can directly impact patient outcomes. Balancing these competing priorities has become increasingly complex as AI systems rely on vast datasets and interdisciplinary cooperation, raising important questions about how to encourage innovation without restricting the flow of knowledge that drives technological advancement [17].

Conclusion

The use of artificial intelligence in healthcare gives rise to a complex set of bioethical and legal challenges that demand critical reflection and a multidisciplinary approach. From a bioethical perspective, AI brings renewed attention to fundamental principles such as autonomy, beneficence, nonmaleficence, and justice, particularly in light of risks related to algorithmic opacity, discriminatory biases, and potential impacts on the doctor–patient relationship. Legally, the Brazilian framework is anchored primarily in the LGPD, which establishes strict safeguards for the processing of sensitive data, complemented by the regulatory actions of the ANPD that aim to ensure safety, efficacy, and accountability in the clinical use of automated systems. The convergence of these regulatory pillars demonstrates that the ethical and legally sound adoption of AI in healthcare depends on governance mechanisms that promote transparency, meaningful human oversight, and the full protection of fundamental rights, ensuring that technological innovation does not override dignity or equity in health care.

The future of healthcare supported by artificial intelligence can be conceived as a horizon in which technology and human values no longer operate as opposing forces, but instead function in a complementary manner to promote a more comprehensive understanding of health and wellbeing. Rather than replacing human professionals, intelligent systems have the potential to expand clinical capacities for care, anticipation, and interpretation of complex biological and social phenomena. In such a scenario, AI is not merely an instrument of operational efficiency; it becomes an ethically aligned tool capable of transforming data into clinically relevant knowledge, shifting the focus from reactive diagnosis to proactive prevention, and contributing to more humane therapeutic experiences.

References

1. Holzinger A, Langs G, Denk H, Zatloukal K, Müller H (2019) Causability and explainability of artificial intelligence in medicine. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 9(4): e1312.

2. Topol EJ (2019) High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine 25: 44-56.

3. Bohr A, Memarzadeh K, Gerke S, Minssen T, Cohen IG (2020) Ethical and legal challenges of artificial intelligence-driven healthcare. In: Artificial Intelligence in Healthcare. Academic Press, pp. 283-314.

4. World Health Organization (2021) Ethics and governance of artificial intelligence for health: WHO guidance. World Health Organization.

5. Associação Brasileira de Normas Técnicas (2023) ABNT NBR ISO/IEC 22989:2023 – Tecnologia da informação — Inteligência artificial — Conceitos e terminologia. ABNT.

6. Senado Federal (2023) Projeto de Lei nº 2.338, de 2023: Dispõe sobre o uso da Inteligência Artificial. Senado Federal, Brazil.

7. Ministério da Ciência, Tecnologia e Inovações (2021) Estratégia Brasileira de Inteligência Artificial – EBIA. Secretaria de Empreendedorismo e Inovação, Brazil.

8. Ministério da Ciência, Tecnologia e Inovação – MCTI, Centro de Gestão e Estudos Estratégicos – CGEE (2025) IA para o bem de todos: Plano Brasileiro de Inteligência Artificial. MCTI; CGEE, Brazil.

9. Elias MA, Faversani LA, Moreira JAV, Masieiro AV, Bellinati NVC (2023) Inteligência artificial em saúde e

implicações bioéticas: Uma revisão sistemática. Revista Bioética 31(3): 1-12.

10. Obermeyer Z, Powers B, Vogeli C, Mullainathan S (2019) Dissecting racial bias in an algorithm used to manage the health of populations. Science 366(6464): 447-453.

11. Singh RR, Garg A (2025) Evaluating IBM Watson's role in oncology treatment decisions: A case study on AI-based clinical decision support. Hematological Disorders in the Single-Cell Era 1(2).

12. Hassija V, Chamola V, Mahapatra A, Singal A, Goel D, et al. (2024) Interpreting black-box models: A review on explainable artificial intelligence. Cognitive Computation 16(1): 45-74.

13. Health Insurance Portability and Accountability Act of 1996 (1996) Pub. L. No. 104-191, 110 Stat. 1936.

14. Balcioğlu YS, Çelik AA, Altindağ E (2025) A turning point in AI: Europe's human-centric approach to technology regulation. Journal of Responsible Technology 23.

15. Mohurle S, Patil M (2017) A brief study of WannaCry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science 8(5).

16. Brasil (2018) Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Brazil.

17. Cuntz A, Fink C, Stamm H (2024) Artificial intelligence and intellectual property: An economic perspective. World Intellectual Property Organization.