JOURNAL OF THE INDIAN LAW INSTITUTE

VOLUME 66 APRIL-JUNE 2024 NUMBER 2

ETHICO-LEGAL PERSPECTIVES ON THE IMPACT OF ARTIFICIAL INTELLIGENCE ON MEDICAL DATA PRIVACY

Ashwini Siwal[*]
Jayanta Ghosh[**]

Abstract

The potential for better diagnosis, treatment, and patient outcomes is enormous, making the application of artificial intelligence (AI) in healthcare a game-changer. However, this paradigm change raises complex ethical and legal questions, especially in regards to the protection of sensitive medical information. This study delves into and analyses important aspects of the legal and ethical framework around AI in medical data, stressing the need to strike a balance between the two. Background is provided in the introduction, with an emphasis on the expanding use of AI in healthcare and the rising tensions over its potential effects on personal privacy. The statement of problem establishes the tone for a thorough investigation by emphasising the urgent necessity to deal with the ethical and legal issues. The first part, "Data Sensitivity and Informed Permission," delves into ethical worries about the confidentiality of medical records and the fallout from insufficient informed consent. At the same time, the requirements for explicit consent in the processing of medical data as outlined by regulations like the General Data Protection Regulation (GDPR) are investigated. The second portion, "Algorithmic bias and fairness," delves into the moral issues raised by the existence of inherent biases in AI algorithms and what those biases mean for the promotion of fairness and equity in clinical decision-making. Compliance with anti-discrimination legislation and mandates for auditing and reducing biases are essential parts of the legal system. The third section, "Security and Data Breaches,"

* Course Coordinator, Certificate Course on Patents, Research Council, University of Delhi and Assistant Professor, Faculty of Law, University of Delhi.

** Head and Research Fellow, Centre for Regulatory Studies, Governance and Public Policy, West Bengal National University of Juridical Sciences, Kolkata.

addresses the moral quandaries caused by the increasing exposure of medical data as a result of AI integration, as well as the legal requirements for securing and disclosing such breaches. The fourth section, titled "Openness and Explainability," examines the ethical problems associated with the lack of transparency in AI decision-making and the significance of people being able to comprehend and trust AI-driven medical judgments. Transparency and accountability requirements of the law are discussed. The fifth section, "Data Ownership and Control," looks at patient expectations, potential conflicts caused by AI-driven insights, and legislative requirements addressing data ownership and control rights. It highlights the importance of striking a compromise between protecting patients' privacy and facilitating medical progress. The sixth part, titled "De-identification and Anonymization," delves into the moral issues surrounding the protection of personal information throughout the de-identification process and the dangers of subsequent re-identification. Methods for continual evaluation and the legal requirements for effective de-identification are presented. In conclusion, briefly review the most important ethical and legal considerations, and a middle ground that prioritises people's values and privacy when it comes to AI-powered healthcare are argued. In order to successfully negotiate this complicated convergence, the paper stresses the importance of continual collaboration amongst stakeholders in technology, ethics, law, and healthcare.

I Introduction

IN RECENT times, there has been a notable increase in the utilisation of artificial intelligence (AI) applications within the healthcare industry.[1] These applications encompass a wide range of functions, including diagnostic tools and personalised treatment regimens. Artificial intelligence (AI) has exhibited the capacity to augment the effectiveness of medical procedures, optimise diagnostic procedures, and enhance patient results through the analysis of extensive datasets at a rate surpassing human capabilities. The integration of AI algorithms into many clinical practises is becoming more prevalent, hence enhancing the precision of disease detection, prognosis, and therapy recommendations. The sensitivity of medical data lies in its inherent nature, as it encompasses a range of personal health records, treatment histories, and genetic information.[2] The use of artificial intelligence presents the dilemma of ensuring the

1 A., Bohr, and K. Memarzadeh, "The rise of artificial intelligence in healthcare applications." In *Artificial Intelligence in healthcare Academic Press* 25-60 (2020).

2 W. N. Price and I. G. Cohen,"Privacy in the age of medical big data" 25(1) *Nature medicine* 37-43(2019).

protection of this exceedingly sensitive data. The extensive availability and utilisation of medical datasets in AI systems give rise to concerns regarding the possibility for misuse, unauthorised access, or inadvertent exposure of sensitive patient information. The increasing dependence on AI in the healthcare sector gives rise to apprehensions among individuals regarding the management of personal medical data, thereby raising inquiries about the level of confidence in healthcare systems and the ethical implications associated with data privacy.

It is imperative to consider the ethical and legal ramifications of AI in relation to the privacy of medical data, as this is essential for maintaining a harmonious equilibrium between technical progress and fundamental human principles.[3] The ethical aspect encompasses the evaluation of the influence of AI on the rights and autonomy of persons, as well as the safeguarding of human values, particularly in relation to sensitive medical data. The legal standpoint places significant emphasis on adhering to current data protection legislation, implementing informed consent procedures, and formulating novel policies to effectively tackle the distinct issues presented by AI in the healthcare domain. The research posits the necessity of achieving a nuanced equilibrium between harnessing the advantages of AI in the realm of medical progress and safeguarding the principles of personal privacy, well-informed choices, and ethically sound healthcare methodologies.[4] To uphold public confidence in the healthcare system, it is crucial to conduct a thorough examination of the ethical and legal aspects. This examination ensures that individuals can trust that their medical information is managed in a responsible manner, adhering to established ethical and legal standards. Ethico-legal issues serve as a guiding framework for developers, policymakers, and healthcare practitioners, facilitating the responsible development and implementation of AI technology within medical contexts.[5] This study highlights the importance of maintaining essential human values, such as privacy, autonomy, and dignity, in light of ongoing technological breakthroughs that are transforming the healthcare sector. The introductory section of the text establishes a context by emphasising the significant impact of AI in the healthcare sector, while simultaneously recognising the urgent issues pertaining to the safeguarding of data privacy. The research statement posits that an ethico-legal viewpoint is essential for effectively navigating the complex landscape of AI in medical data. This perspective is crucial for achieving a balanced coexistence between technical advancements and human values.

3 T. Tzimas, "Legal and Ethical Challenges of Artificial Intelligence from an International Law Perspective" *Springer Nature* 46 (2021).

4 D. Leslie, "Tackling COVID-19 through responsible AI innovation: Five steps in the right direction" *Harvard Data Science Review* 10 (2020).

5 A. A. Jogi, *Artificial intelligence and healthcare in South Africa: ethical and legal challenges* (Doctoral dissertation) (2021).

II Data sensitivity and informed consent

The domain of medical data covers information of a highly personal and sensitive nature, which includes intricate particulars of an individual's health conditions, treatments, drugs, and genetic composition. The incorporation of AI into healthcare procedures amplifies apprehensions regarding the possible encroachment upon privacy, given the more advanced and extensive analysis of medical data.[6] The potential disclosure of confidential medical information in the absence of adequate measures can result in psychological distress, social stigma, and discriminatory treatment. This underscores the ethical obligation to ensure the confidentiality of such data. The concept of informed consent is a fundamental principle in the realm of ethical medical practises, serving as a means to guarantee that individuals possess the capacity to exercise their autonomy in making informed choices regarding the use of their medical information. Insufficient or ambiguous consent procedures undermine the confidence between patients and healthcare practitioners, giving rise to apprehensions over the transparency and ethical use of confidential data.[7] In the absence of explicit consent, individuals may remain uninformed regarding the manner in which their data is employed, hence resulting in inadvertent ramifications such as the utilisation of data for purposes that were neither anticipated nor authorised.

The General Data Protection Regulation (GDPR) is a prominent legal framework that primarily aims to safeguard personal data, including medical information, inside the boundaries of the European Union.[8] The General Data Protection Regulation (GDPR) delineates the fundamental principles of lawfulness, fairness, and transparency in the processing of data, with a particular emphasis on the requirement of obtaining explicit agreement when dealing with sensitive data. The legal framework affords individuals the entitlement to get information on the handling of their data, underscoring the significance of providing clear and understandable information during the process of obtaining consent. In accordance with legal regulations, it is required that consent for the processing of medical data be characterised by clarity, specificity, and lack of ambiguity, thereby guaranteeing that persons possess a comprehensive understanding of the purpose and extent of data utilisation.[9] The

6 K. E. Karches, "Against the I Doctor: why artificial intelligence should not replace physician judgment" 39(2) *Theoretical Medicine and Bioethics* 91-110 (2018).

7 M. J. Taylor, "Legal bases for disclosing confidential patient information for public health: distinguishing between health protection and health improvement" *23*(3) *Medical Law Review*, 348-374 (2015).

8 Paul Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)" *A Practical Guide,* 1st edn., *Cham: Springer International Publishing*, 10 (3152676), 10-5555(2017).

9 L. A. Bygrave, "Data protection by design and by default: deciphering the EU's legislative requirements" 4(2) *Oslo Law Review* 105-120(2017).

General Data Protection Regulation (GDPR) sets down criteria for permission to be considered valid, encompassing elements such as voluntary participation, adequate information provision, and the right to withdraw consent at any given moment. These requirements serve to strengthen the ethical values of autonomy and the recognition of individuals' decision-making authority. The legislative framework promotes continuous communication between data controllers and individuals, facilitating transparent disclosure of any modifications in data processing practises. This enables individuals to exercise their right to exert control over their data. The ethical considerations pertaining to the sensitivity of medical data and the requirement for informed consent are in accordance with regulatory frameworks such as the General Data Protection Regulation (GDPR), highlighting the pivotal significance of express consent in the handling of medical information.[10] The aforementioned dual perspective highlights the necessity of implementing ethical and legal measures in order to guarantee the rights and privacy of individuals within the context of AI-driven healthcare.

III Algorithmic bias and fairness

AI systems have the potential to unintentionally acquire and sustain biases that exist within the training data, so mirroring societal prejudices or systematic inequalities.[11] The presence of biases in AI systems can give rise to variations in diagnosis and treatment suggestions, which may consequently give rise to disparities in healthcare results. These discrepancies can be attributed to factors such as race, gender, or socioeconomic position. The examination of biases poses a significant challenge to the credibility of AI systems, since it prompts individuals to question the impartiality and dependability of automated medical decision-making. Algorithmic biases have the potential to play a role in the persistence of healthcare disparities, hence amplifying inequalities in the availability of high-quality healthcare services and perpetuating historical injustices.[12] Recommendations for addressing unfair treatment can have a significant impact on the results of patients, thereby undermining the fundamental principles of medical ethics that prioritise equitable access to healthcare and the obligation to prevent discriminatory practises. The presence of biased algorithms poses a hindrance to patients' ability to engage in informed decision-making, hence undermining their capacity to make choices grounded in unbiased and evidence-based information.

10 E. S. Dove, "The EU general data protection regulation: implications for international scientific research in the digital era. 46(4) *Journal of Law, Medicine and Ethics*, 1013-1030 (2018)".

11 U. Peters, Algorithmic political bias in artificial intelligence systems. 35(2) *Philosophy & Technology* 25 (2022).

12 S. Hoffman, and A. Podgurski, "Artificial intelligence and discrimination in health care" 19 *Yale J. Health Pol'y L. and Ethics* 1 (2019).

Legal frameworks may impose obligations on AI developers and healthcare providers to incorporate mechanisms for conducting audits and promoting openness in AI systems, so enabling the detection and correction of biases.[13] Regular audits and monitoring play a crucial role within the legal framework, facilitating continuous examination of AI systems in order to identify and rectify biases as they arise. Legal obligations may necessitate the documentation and reporting of endeavours to alleviate biases, so promoting accountability and openness in the implementation of artificial intelligence in the healthcare sector. The incorporation of prevailing anti-discrimination laws and regulations within the legal framework governing artificial intelligence (AI) in the healthcare sector is imperative in order to mitigate the potential for biased algorithms to perpetuate discriminatory practises. Legal standards may establish requirements that necessitate AI systems to refrain from engaging in discriminatory practises on the basis of protected characteristics, including but not limited to race, gender, age, or disability.[14] These standards are in line with wider endeavours aimed at eradicating biases within decision-making procedures. Non compliance with anti-discrimination laws can lead to legal ramifications, hence emphasising the significance of ensuring that AI practises in healthcare adhere to ethical standards of justice and equity. To effectively tackle algorithmic prejudice and uphold justice in AI-driven medical decision-making, it is imperative to adopt a comprehensive approach that integrates ethical considerations alongside legal safeguards.[15] The ethical considerations underscore the possible ramifications on society that arise from algorithms that exhibit bias. Simultaneously, the legal framework underscores the importance of openness, accountability, and adherence to anti-discrimination legislation in order to foster healthcare outcomes that are fair and just.

IV Security and data breaches

The incorporation of AI into healthcare systems presents novel vulnerabilities and broadens the potential targets for attacks, as AI applications frequently necessitate access to huge collections of medical data.[16] AI technologies, although they enhance the capabilities of healthcare, also present themselves as possible targets for advanced cyber threats, hence increasing the vulnerability of sensitive medical data. The heightened susceptibility gives rise to ethical considerations about the preservation of patient confidence in healthcare establishments, particularly when individuals rely

13 P. Almeida, C. D. dos Santos, *et.al.*, "Artificial intelligence regulation: a framework for governance." *23*(3) *Ethics and Information Technology*, 505-525.

14 A. Prince and D. Schwarcz, "Proxy discrimination in the age of artificial intelligence and big data" *105 Iowa L. Rev.* 1257(2019).

15 S. Gerke, T. Minssen *et.al.*, "Ethical and Legal Challenges of Artificial Intelligence-Driven Healthcare" in *Artificial Intelligence in Healthcare* (Academic Press 295-336 2020).

16 Sandip Reddy, Sonia Allan, *et. al.,* "A governance model for the application of AI in health care" 27(3) *Journal of the American Medical Informatics Association* 491-497 (2020).

on AI-powered technologies to handle their confidential health data. The act of gaining unauthorised entry to medical data constitutes a significant violation of privacy, hence subjecting persons to potential risks such as identity theft, discrimination, and other adverse outcomes. Data breaches in the healthcare system can have a detrimental impact on trust, as patients may begin to doubt the institutions' capacity to effectively protect their sensitive information. Consequently, this may result in patients being hesitant to seek medical care or disclose crucial health information. The ethical aspect encompasses the potential negative consequences that may arise for individuals whose medical data is compromised, as unauthorised access can result in misdiagnoses, inappropriate treatment, or other unfavourable consequences. Numerous legislations pertaining to data protection, such as the General Data Protection Regulation (GDPR), delineate precise stipulations aimed at safeguarding personal and sensitive data, including medical records.[17] Healthcare institutions and AI developers are required by the regulatory framework to incorporate strong cybersecurity measures, such as encryption, access limits, and routine security assessments, in order to protect against any data breaches. Legal regulations may also prioritise the principle of data minimization, promoting the acquisition and preservation of solely essential medical information in order to mitigate the potential consequences of breaches.

Data protection regulations frequently have measures that necessitate the prompt and open disclosure of data breaches to pertinent regulatory bodies and impacted persons.[18] Legal regulations often provide specific standards that dictate the procedures for informing persons whose personal data has been compromised. This ensures that affected individuals are promptly notified, allowing them to take proactive steps to safeguard their personal information. Non compliance with reporting requirements can lead to legal ramifications, emphasising the importance of upholding transparency and accountability following a data breach.[19] The ethical considerations pertaining to the heightened susceptibility of medical data resulting from the integration of artificial intelligence (AI) are closely linked to legal responsibilities aimed at safeguarding confidential information. The legislative framework places significant emphasis on proactive cybersecurity measures, obligatory reporting, and transparent communication in the occurrence of data breaches. This alignment of ethical standards with the necessity for legal safeguards aims to secure persons and uphold faith in the healthcare system.

17 D. Mendelson, "Legal protections for personal health information in the age of Big Data–a proposal for regulatory framework" 3(1) *Ethics, Medicine and Public Health,* 37-55. (2017).

18 P. M. Schwartz, and E. J. Janger, "Notification of data security breaches" 105 *Mich. L. Rev.*, 913(2006).

19 A. Daly, "The introduction of data breach notification legislation in Australia: A comparative view" 34(3) *Computer Law and Security Review* 477-495(2018).

V Transparency and explainability

Artificial intelligence systems, especially those employing deep learning and intricate neural networks, possess a characteristic of opacity and provide challenges in interpretation, hence impeding comprehension of the decision-making process. The lack of explainability associated with certain AI models, characterised by their black-box nature, gives rise to worries over humans' limited capacity to comprehend the underlying logic behind medical decisions. The ethical implications arising from the opacity of decision-making processes in AI give rise to concerns regarding responsibility, trust, and the possibility of biased or unjust outcomes in the absence of transparent systems. The ethical standards governing healthcare underscore the need of patients making informed decisions. The absence of transparency in AI systems has the potential to impede users' capacity to make informed judgements due to a limited comprehension of the underlying processes.[20] The establishment of transparent AI decision-making processes is of utmost importance in fostering and preserving confidence within the realm of healthcare, both among individuals and healthcare professionals. Trust is a fundamental aspect of healthcare partnerships, and the absence of openness has the potential to undermine this trust. Ethical healthcare practices prioritise patient autonomy, since individuals who possess a comprehensive grasp of AI-driven decisions are empowered to actively engage in their healthcare, hence cultivating a heightened sense of control and autonomy.[21]

Legal frameworks sometimes incorporate explicit regulations that require transparency and explainability to be upheld during the process of developing and using AI systems within the healthcare sector.[22] Legislation may mandate that establishments provide public access to information pertaining to the operational mechanisms of artificial intelligence algorithms, so guaranteeing transparency regarding the influence of this technology on medical decision-making. Legal norms can potentially incorporate the notion of algorithmic responsibility, thereby imposing obligations on developers and healthcare providers to ensure the transparency of AI systems in order to address ethical considerations. Legal mechanisms can be employed to ensure adherence to transparency norms, necessitating those entities conduct periodic audits and divulge information pertaining to the operations of artificial intelligence algorithms employed within medical domains. Legal frameworks have the potential to bestow upon patients

20 U. Ehsan, Q. V. Liao, *et.al.,* "Expanding explainability: Towards social transparency in ai systems" in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems 1-19 (2021).

21 A. Boch, S. Ryan, *et.al.,* "Beyond the Metal Flesh: Understanding the Intersection between Bio-and AI Ethics for Robotics in Healthcare" 12(4) *Robotics* 110(2023).

22 *Supra* note 16.

the entitlement to obtain comprehensible explanations for decisions influenced by artificial intelligence (AI) that impact their healthcare.[23] This serves to strengthen the ethical ideal of upholding patient rights. The absence of compliance with transparency and explainability standards might result in legal ramifications, underscoring the significance of accountability in the implementation of AI systems within the healthcare sector. The ethical and legal dimensions of AI-driven medical judgements necessitate the utmost importance of transparency and explainability. Ethical considerations revolve around the promotion of individual empowerment, the preservation of trust, and the protection of patient autonomy. In contrast, the legal framework places emphasis on regulatory obligations and measures of accountability to guarantee transparency in AI systems, thereby matching technological progress with ethical values within the healthcare domain.

VI Data ownership and control

When patients offer consent to share their medical data with healthcare practitioners, they frequently develop a perception of ownership and control over this information.[24] Ethical considerations emerge when these expectations are not fulfilled. Ethical healthcare practises place significant emphasis on the fundamental values of trust and transparency. Patients may experience a sense of betrayal upon discovering that their medical data is being utilised in manners that were not anticipated or without obtaining their explicit consent.[25] The ethical principle of patient autonomy emphasises the entitlement of individuals to exercise control over the disclosure and access of their medical information. The potential impact of AI-driven insights on patient autonomy necessitates a thorough examination of patient expectations. The utilisation of AI to derive insights has the potential to produce interpretations of medical data that may diverge from patients' preconceived notions or personal convictions on their health issues. The ethical challenges associated with the management of these conflicts are considerable. The possible discord between AI-generated insights and patient expectations has the potential to create tension within doctor-patient relationships, which may result in compromised communication and diminished trust. Ethical issues encompass the delicate task of striking a harmonious equilibrium between the advantages derived from AI-powered insights in the realm of medical progress and

23 A. R. Kunduru, "Machine Learning in Drug Discovery: A Comprehensive Analysis of Applications, Challenges, and Future Directions" 5(8) *International Journal on Orange Technologies* 29-37(2023).

24 K. Liddell, D. A. Simon, "A Patient data ownership: who owns your health?" 8(2) *Journal of Law and the Biosciences*, lsab023(2021).

25 C. S. Bond, O. H. Ahmed, "The conceptual and practical ethical dilemmas of using health discussion board posts as research data" 15(6) *Journal of medical Internet research*, (2013).

the possible hazards associated with the divergence from patient expectations and values.[26]

Legal frameworks often provide individuals with the entitlement to access, edit, or potentially delete their medical data. This approach enables patients to retain authority over their personal information and is in accordance with ethical ideals of autonomy.[27] The concept of consent continues to hold significant importance within the realm of law. The legal framework may impose a requirement for explicit agreement in the context of utilising artificial intelligence for processing medical data, hence strengthening the ethical value of upholding individuals' autonomy. Certain legal provisions may encompass data portability rights, which grant individuals the opportunity to transfer their medical data from one healthcare provider to another. This provision serves to enhance individuals' control and ownership over their own medical information. Legal systems frequently recognise the significance of medical research and progress. Achieving a harmonious equilibrium between these two aspects necessitates the establishment of unambiguous protocols governing the utilisation of data for the betterment of society, while simultaneously upholding the principles of human ownership and autonomy. Legal norms often prioritise the ethical use of anonymization and de-identification techniques in order to safeguard patient privacy, while yet enabling the utilisation of aggregated data for wider medical research purposes. In certain instances, legal frameworks may take into account the societal benefit of medical progress, thereby establishing a legal foundation for the utilisation of data while safeguarding individual rights from excessive infringement. The ethical considerations pertaining to the ownership and control of data within the realm of AI-generated insights underscore the significance of upholding patient autonomy and effectively addressing any conflicts.[28] The legal framework is of paramount importance in achieving a harmonious equilibrium between leveraging the potential of AI in the healthcare sector and safeguarding the rights and expectations of persons. This is accomplished through the inclusion of regulations pertaining to consent, access rights, and considerations for medical advancements.

VII De-identification and anonymization

The process of de-identification, which involves the removal of personally identifiable information, is not entirely infallible. The presence of complex medical data poses challenges since it may encompass distinctive amalgamations of information that

26 J. M. Puaschunder, "Big data, algorithms and health data" *Algorithms and Health Data* (October 22, 2019).

27 B. Friedman and Jr, P. H. Kahn "Human Values, Ethics, and Design" *The Human-Computer Interaction Handbook* 1177-1201 (2003).

28 C. Wang, S. Liu, *et.al.,* "Ethical considerations of using ChatGPT in Health Care" 25 *Journal of Medical Internet Research,* (2023).

could potentially enable re-identification.[29] The rapid progress in data analytics and AI technology presents significant obstacles in preserving privacy through the process of de-identification. The emergence of ethical concerns arises when medical data, which is presumed to be anonymous, can be potentially re-identified, so violating the privacy of individuals. Healthcare providers and developers of AI have a moral need to incorporate strong de-identification protocols, recognising the potential hazards involved and striving to mitigate them to the greatest extent feasible. The potential re-identification of ostensibly anonymized medical data has the capacity to result in a substantial infringement of privacy. The association between individuals and sensitive health information has the potential to expose them to various risks, including potential injury and prejudice. Instances of re-identification undermine confidence in the effectiveness of de-identification practises and the secure management of medical data. The erosion of trust can have wide-ranging consequences, including individuals' inclination to engage in research endeavours or disclose their personal health data. Ethical considerations encompass the possibility of impeding medical research and progress. The apprehension surrounding the possibility of re-identification has the potential to result in heightened limitations on the sharing of data, so constraining the overall advantages that can be obtained from research endeavours. Legal frameworks often establish explicit recommendations regarding the de-identification and anonymization of medical data, delineating the precise procedures and criteria that must be adhered to in order to safeguard human privacy.[30] Certain legislative norms are in accordance with international frameworks that specify optimal methods for de-identification and anonymization, thereby upholding a worldwide dedication to safeguarding the privacy of patients.

Legal frameworks often include the incorporation of the idea of differential privacy. This concept involves the addition of noise to data in order to safeguard individual identities, while still enabling meaningful analysis.[31] By integrating differential privacy, the efficiency of de-identification methods is enhanced. Healthcare organisations and AI developers may have a legal duty to regularly evaluate the efficacy of de-identification techniques in response to improvements in technology and the emergence of new re-identification concerns. The legal framework may require the integration of technology advancements and innovations in order to bolster the security of de-identified data, thereby acknowledging the ever-evolving nature of privacy concerns. Legal standards encompass several accountability measures, including but not limited

29 A. Drozdz, *Protection of Natural Persons with Regard to Automated Individual Decision-Making in the GDPR*, (Kluwer Law International 2020).

30 J. Polonetsky, O. Tene *et.al.,* "Shades of gray: Seeing the full spectrum of practical data de-intentification" 56 *Santa Clara L. Rev.* 593(2016).

31 C. Li and B. Palanisamy, "Privacy in internet of things: From principles to technologies" 6(1), *IEEE Internet of Things Journal* 488-505(2018).

to frequent audits and reporting obligations. These procedures are implemented to ascertain that companies responsible for managing medical data are diligently engaged in safeguarding patient privacy by employing appropriate de-identification practises. The ethical considerations pertaining to the processes of de-identification and anonymization underscore the significance of recognising the constraints and possible hazards inherent in these methodologies.[32] The primary objective of the legislative framework is to achieve a harmonious equilibrium between the utilisation of medical data for research and innovation, and the protection of patient privacy. This is accomplished by the establishment of explicit standards and the implementation of ongoing evaluation criteria. Furthermore, the legal framework also endeavours to tackle the ever-changing obstacles associated with re-identification.

VIII Conclusion

The GDPR-compliant ethical requirement of express informed consent for sensitive medical data processing. Addressing AI algorithm biases to promote fairness and equity in medical decision-making with legal audits and mitigation requirements. AI integration raises ethical concerns regarding medical data security, as well as regulatory requirements for strong cybersecurity and data breach notification. Ethics connected to AI decision-making openness and the need of understanding and trusting AI-driven medical judgements, reinforced by legislative transparency and accountability obligations. Ethical issues surrounding patient expectations, AI-driven insights, and data ownership and control rights, emphasising a balance between technology and patient rights. Legal norms for effective de-identification and continuing method review strengthen ethical concerns regarding privacy and re-identification hazards. Accepting the ethical obligation to prioritise patient autonomy, privacy, and trust in healthcare AI implementation. Recognising the relevance of legal frameworks in setting clear norms, guaranteeing responsibility, and balancing AI-driven medical advances with individual rights. A patient-centric strategy that prioritises human values and privacy in medical AI development and application. Recognising the complexity of ethico-legal issues involving AI in medical data and encouraging collaboration amongst technology specialists, ethicists, lawyers, and healthcare practitioners. Promoting open conversation between stakeholders to address developing ethical and legal issues, adapt to technological advances, and keep rules current and effective. Promoting ethical AI technology development with a focus on transparency, justice, and patient privacy. Advocate for education and awareness programme to enlighten healthcare professionals and the public about the ethico-legal implications of AI in medical data to promote informed decision-making and responsible AI practises. Medical AI, data privacy, and human values demand a holistic and collaborative

32 D. Florea and S. Florea, "Big Data and the Ethical Implications of Data Privacy in Higher Education Research" 12(20) *Sustainability* 8744(2020).

approach. The healthcare ecosystem may use AI while respecting human values and privacy rights by embedding ethical concepts into legislative frameworks, increasing stakeholder engagement, and focusing on patients.