Science of Law, 2024, No. 4, pp. 8-14
DOI: 10.55284/

Artificial Intelligence: Legal and Ethical Perspectives in the Health Care Sector

Mohammad Owais Farooqui[1]*, Tahir Qureshi[2], Nazzal Kisswani[3], Dhananjay Kumar Mishra[4]

[1]Department of Public Law, College of Law University of Sharjah, Sharjah, United Arab Emirates.
[2]Symbiosis International (Deemed University), Pune, Hyderabad Campus, India.
[3]Department of Private Law, College of Law, University of Sharjah, Sharjah, United Arab Emirates.
[4]Symbiosis Law School, Hyderabad Campus, Symbiosis International (Deemed University), Pune, India.

Keywords:
Artificial intelligence;
Data privacy and security;
Ethical challenges;
Healthcare sector;
Informed consent;
Legal frameworks.

Article history:
Received: 08/11/2024
Revised: 10/12/2024
Accepted: 20/12/2024

Abstract. In this study, the researchers aim to establish how Artificial Intelligence (AI) has revolutionized the health care industry and the ethical and legal issues pertaining to the use of such technology in this organization. The study provides recommendations for implementing value-adding measures to ensure the safe, secure, and ethical use of AI in healthcare, as well as addressing important concerns and providing solutions to effectively implement AI. Using a quantitative research design, the study uses primary and secondary data to critically analyze relevant literature and existing information. It highlights key challenges that come about because of the current boundaries of regulating AI in healthcare, including but not limited to informed consent, transparency, privacy, data protection, and fairness. The study is fundamentally important to the theory and practice of the implementation of AI technologies, as it illustrates the high potential of using them in the sphere of patient care and, at the same time, cites significant ethical and legal issues in their application. To fully achieve the rightly hailed benefits of AI in health care, we must address these issues. To use the AI components responsibly, rules and regulations of ethical and legal standards must change to accommodate key concerns such as consent, ownership, disclosure, and bias. These measures are critically important to centralize patient rights protection and build confidence in health care organizations. Consequently, this study offers practical policy implications that policymakers, healthcare practitioners, and technologists should consider when implementing regulatory policies. Thus, on one hand, such frameworks allow bringing innovation into the field of healthcare by AI while, on the other hand, maintaining compliance to guarantee that such solutions will be both effective and fair.

1. INTRODUCTION

Artificial Intelligence (AI) is a change-oriented and universal approach that is revolutionizing every field and activity of people's lives. Renowned scientist Stephen Hawking said that it was either the best or the worst thing to happen to humanity, and it has emerged in its developed form. Following similar remarks, John Roberts, current Chief Justice of the United States Supreme Court, urged the public to be careful and reserved in addressing the issue of AI advancement (Reuters, 2024). In this regard, advancing a complete and fair legal regulation for applied AI technologies has become an urgent necessity.

But the healthcare sector is where AI technologies are most visible, as they have transformed diagnosis, treatment, and care. However, the integration of AI in healthcare has presented both opportunities and challenges, including detailed accountability issues, algorithmic bias, and transparency in decision-making, and intellectual property rights (IPR). The lack of a comprehensive global strategy to address these ethical and legal concerns poses significant challenges (Krishnan Ganapathy, 2021). Therefore, it is crucial to subject the designs of AI systems in healthcare to professional ethical standards and value systems while also holding developers and stakeholders accountable for their work.

Although some countries have begun to develop AI regulations in the healthcare sector, the advancements remain modest. The European Union (EU)—an absolute leader in this area—introduced the world's first horizontal legal framework for the regulation of AI. The EU framework comprises extensive regulations on data quality, transparency, human involvement, and responsibility norms, backed by some of the precedent-setting legislation, such as the General Data Protection Regulation (GDPR), the Digital Services Act, the Digital Markets Act, and the Artificial Intelligence Act of 2023 (Parliament, 2023). However, many EU member states maintain separate national policies on AI, reflecting diverse approaches to regulation (Labhaoise & Fhaoláin, 2020).

The United States has also taken measures to address the risks and challenges posed by AI. Under the Obama administration, efforts to study and regulate AI began in earnest, with the National Science and Technology Council setting benchmarks for AI research in 2016 (Lyons, 2016). Subsequently, the *National Defense Authorization Act* of 2018 established the *National Security Commission on Artificial Intelligence* to examine security measures and strategies for AI development (UNT, 2021). In 2019, the White House's Office of Science and Technology Policy introduced a draft *Guidance for Regulation of AI Applications*, outlining ten principles for federal agencies to consider when regulating AI (Tech, 2020). The Biden administration further advanced these efforts by announcing an executive order on October 30, 2023, focused on ensuring the safe, secure, and trustworthy use of AI (House, 2023a).

In the United Kingdom, a *Pro-Innovation Approach to AI Regulation* white paper, released in 2023, outlines key principles for AI governance while allowing sector-specific authorities significant latitude to tailor regulations to industries such as financial markets and transportation (Conversation, 2023). Additionally, the UK's Medicines and Healthcare products Regulatory Agency (MHRA) introduced a *Medical Device Change Programme* roadmap to address AI-related challenges in medical devices, focusing on providing guidance and filling gaps in existing regulations (Catherine Bushen, 2023).

The global landscape of AI regulation remains fragmented, with each jurisdiction adopting measures suited to its unique priorities. However, as AI continues to evolve, coordinated international efforts will be essential to address its ethical and legal challenges comprehensively.

2. LITERATURE REVIEW

This literature review aims to establish the following gaps within the body of the literature regarding the problems related to the adoption of AI in the healthcare industry. The literature reviewed proves that the lack of perfect regulation and the practical application of AI are still

*Corresponding author.

issues (Gerke, Minssen, & Cohen, 2020). Despite the increasing focus on AI in healthcare, there remains a lack of understanding regarding its regulation, the innovation in its implementation processes, and the most efficient ways to integrate it into the sector (Naik et al., 2022).

Several studies have discussed the transformative potential of AI in healthcare. For instance, Gerke et al. (2020) highlight the ethical and legal challenges associated with AI-driven healthcare, emphasizing the need for comprehensive frameworks to address transparency, fairness, and accountability. Similarly, Price (2017) identifies the implications of AI applications on data privacy and intellectual property in healthcare, noting gaps in existing legal structures. Furthermore, Naik et al. (2022) underline the necessity of creating new legal classifications for AI phenomena, which challenge traditional legal frameworks.

Data protection has been a major concern in AI applications. Cai (2021) discusses strategies to safeguard health data and mitigate risks related to its secondary use. This concern aligns with insights from the European Union's General Data Protection Regulation (GDPR), which sets stringent rules for data processing and security (European Union, 2016). Comparatively, the fragmented approach in the United States—with laws like HIPAA and COPPA—illustrates the need for a cohesive regulatory framework (Cohen, 2018).

Algorithmic bias is another critical issue explored in the literature. Vyas (2020) and Clifton (2023) highlight instances where biased algorithms have led to discriminatory outcomes, emphasizing the importance of addressing these biases during the development and deployment stages. Moreover, Seyyed-Kalantari, Zhang, McDermott, Chen, and Ghassemi (2021) discuss underdiagnosis bias in AI applications, particularly in underserved patient populations, further underscoring the need for equity in healthcare.

Thus, the purpose of this paper is to provide a critical evaluation of prior research on the benefits of deploying AI applications and the problems encountered in the healthcare industry. Moreover, it examines the unexplored areas to fully harness AI's potential in this particular business sector. By filling these gaps, this study contributes to the creation of a sound framework for ethical, efficient, and sustainable AI application in healthcare.

3. RESEARCH METHOD

The current research utilizes a qualitative research paradigm to explore the topic of AI in the healthcare industry. Previous studies cited in the research were also subjected to a critical analysis to determine gaps that were not well explored in the previous literature in developing an understanding of the challenges and opportunities of this field with the incorporation of AI solutions.

The researchers used primary and secondary data collection techniques to produce the most adequate results. The primary sources were the legal documents, the construction of which formed the basis of the framework for regulating constructions in the area of interest, while the secondary sources included scientific articles and reports, recent publications, and articles found in scientific journals. The identified approach facilitated the critical integration of existing knowledge and highlighted significant gaps that require attention to enhance the application of AI in the healthcare sector.

3.1. Theoretical Framework

Artificial intelligence has finally found its place in the global sphere and is ripening to become one of the most important breakthroughs in healthcare. Right from diagnosis and prognostic tools to precision medicine, virtual assistants, telemedicine, drug development, clinical decision support, and even research, AI's utility is propelling a new face of transformation in healthcare. These innovations have made work easier and can expand to improve the healthcare system across the globe (Price, 2017).

The theoretical foundation of this study is grounded in existing frameworks that assess the ethical, legal, and practical challenges of AI integration in healthcare. Gerke, Minssen, and Cohen (2019) provide a comprehensive analysis of ingestible electronic sensors, addressing the intersection of technology, ethics, and law. Additionally, Naik et al. (2022) emphasize the importance of accountability and transparency in AI systems, arguing for robust legal mechanisms to ensure ethical compliance.

The GDPR is a cornerstone in the data protection discourse, offering a model for safeguarding patient privacy and ensuring data security (European Union, 2016). Comparatively, HIPAA in the U.S. provides a narrower scope, which, as Cohen (2018) points out, leaves significant gaps in non-medical health-related data protection. These legal frameworks inform the development of AI policies that balance innovation with ethical considerations.

Algorithmic bias and equity are pivotal themes in this framework. Vyas (2020) illustrate the impact of racially biased algorithms on healthcare outcomes, while Clifton (2023) proposes adversarial training frameworks to mitigate such biases. The insights of Seyyed-Kalantari et al. (2021) further enrich this discussion, focusing on underdiagnosis biases in marginalized populations.

To ensure ethical and effective AI integration, practitioners must evaluate AI systems against the principles of medical ethics—autonomy, beneficence, non-maleficence, and justice (Markose, 2016). This approach aligns with Nicholson (2016) who emphasizes the necessity of accountability in black-box medicine, and Ronen (2024) who advocates for transparency to build trust and equity in healthcare systems.

This theoretical framework thus provides a multidimensional lens to explore the challenges and opportunities of AI in healthcare, bridging the gaps between technological innovation, ethical considerations, and legal frameworks.

3.1.1. Ethical and Legal Challenges

The application of Artificial Intelligence technologies appears to have unlimited potential in achieving the enhancement of medical education, augmentation of scientific research production, and the improvement of the healthcare system. However, the integration of these technologies has been linked to significant ethical and legal issues, which continue to be a topic of debate today. These issues include the compatibility of AI with current legal frameworks and the necessity to create new legal classifications for AI phenomena that defy traditional legal classifications (Naik et al., 2022).

The cognitive challenges associated with the ethical and legal use of AI technologies include issues such as inconsistent consent, measures and transparency, disproportionality, data security, and proprietary rights. These issues underscore the importance of carefully planning the approaches to AI implementation in healthcare.

Before adopting AI technologies in healthcare, it is imperative that practitioners and specialists rigorously evaluate them against the four fundamental principles of medical ethics: The four principles are autonomy, beneficence, non-maleficence, and justice. It also ensures that the integration of AI will prioritize patients' interests, justice, and trust, thereby facilitating the appropriate application of AI solutions.

3.1.2. Informed Consent

Informed consent emerges as one of the chief ethical concerns as we consider the application of Artificial Intelligence (AI) technologies in

the health care sector. It works as an effective tool helping patients evaluate possible grievances and advantages of their health choices. Based on the principles of medical ethics, which form the foundation of doctor-patient relationships, physicians are required to reveal the potential outcomes of medical treatments and AI solutions.

Patients need clear and unambiguous information about the operations of distinct AI algorithms, their objectives, benefits, drawbacks, impact on privacy, and other related aspects as the use of AI in healthcare expands. Such transparency helps patients make better decisions about using AI in their treatment processes. Due to software sophistication and the unpredictable nature of the results in OMR, such communication could be regarded as critical. The issue of informed consent intensifies when patients fail to comprehend the implications of giving their consent for the use of their data in AI systems, leading to significant concerns regarding data privacy (Moore, 2023).

Ethical responsibility, as described earlier, means that "Patients have the right to be informed on their diagnosis, health status, treatments, therapy results, success rate, test results, costs, insurance share, or other medical facts, and any consent should be specific for purpose, procured freely, and specific." This principle aligns closely with the ethical concept of autonomy (Markose, 2016) ensuring patients retain agency in decisions impacting their healthcare.

Patients also have the unequivocal right to seek detailed information and pose questions regarding medical procedures and treatments. Healthcare professionals must inform patients about the treatment methodology, potential risks associated with processes such as screening and imaging, irregularities in data collection, programming errors, confidentiality concerns, and safeguards surrounding extensive genetic data gathered through testing. Furthermore, healthcare professionals must inform patients about accountability measures in cases of system malfunction or negligence, and they retain the right to refuse therapies deemed appropriate.

Ethical practice, therefore, serves as a foundation to build trust between healthcare providers, AI developers, and patients. Such trust fosters a collaborative healthcare environment that respects individual autonomy, ensures data protection, and promotes the responsible and ethical deployment of AI technologies in the healthcare sector (Vincent, 2024).

3.1.3. Data Protection in Healthcare: Challenges and Global Efforts

Healthcare professionals often describe digital data as a double-edged sword, facilitating advancements in treatment while simultaneously exposing sensitive patient information to potential privacy breaches (Gupta, 2023). Breaches of patient privacy can result in significant harm, including the possibility of discrimination. For instance, if employers or insurers gain unauthorized access to a patient's health data, they may refuse employment or insurance coverage, particularly in cases of severe or critical illnesses (Calo, 2011). Beyond tangible harm, data breaches can cause psychological injuries, such as feelings of shame, anxiety, and distress, which, while not financial in nature, can be deeply detrimental (Nicholson, 2016). Occasionally, big data access to health information can give a person information they did not want to know about another person's health condition (Cohen, 2018).

All these aspects underscore the importance of establishing dependable and efficient data protection frameworks, especially concerning patient information, to avert privacy lapses. Acknowledging these risks, the EU has developed a legal framework through the General Data Protection Regulation (GDPR), which is already applicable across all the EU member states (Wolford, 2020). The GDPR intends to protect individuals' rights to privacy and data protection as provided in Article 1(2). In addition, Articles 2 and 3 of the GDPR describe the processing of personal data within or within the context of the Union and/or outside the EU, including within the United States (European Union, 2016). On the other hand, the United States employs a sectoral approach to legislation, lacking a single comprehensive statute that protects data. The applicable statutes vary depending on the type of information. GLBA pertains to financial information, HIPAA regarding health data, COPPA for data relating to children, and the FTC Act for customer protection. However, these laws lack completeness or contain loopholes. For example, the individual's specific medical record constructed by HIPAA is for the protected data created by a "covered entity" or "business associate" but does not embody non-medical care-related health data like buying pregnancy tests online, which continues to be lawless (Cohen, 2018).

India's data protection policy has undergone modifications due to judicial rulings and newly created laws and legislation. In the recent ruling of the Supreme Court of India, Puttaswamy (Retd.) Justice, Anr, Union of India, and Ors (2017) the Court recognized the right to privacy as a fundamental right. India has just enacted the Digital Personal Data Protection Act (DPDP), 2023, to address escalating dangers related to data protection (Farooqui, Sharma, & Gupta, 2022).

Although people all over the world have now woken up to what data protection entails, the world requires collective effort to tame data and create an environment that will safeguard the sanctity of personal data across the globe. This would not only address current issues in one country but also foster trust in the digital health sector by safeguarding information across borders.

3.1.4. Safety and Transparency in AI Integration in Healthcare

AI systems in health care have raised concerns about safety and explainability, particularly in decision-making. Our primary concern is the transparency and accountability of AI systems, often leading to a lack of understanding of how the systems arrived at a particular decision, a phenomenon known as the 'black box' problem. The ability to recognize AI-produced decisions is critical in numerous important healthcare contexts so as to safeguard patients' welfare and sustain the credibility of healthcare associations.

AI systems allow companies to get a lot of valuable advice based on big data analysis. However, these recommendations may occasionally lead to decisions that deviate from the initial training set, potentially posing risks to trust and safety (Ronen, 2024). AI technologies in machine learning are also capable of reproducing social biases, such as access to quality health care or health insurance. Adoption of these technologies without transparency could potentially exacerbate existing inequalities in the delivery of healthcare services.

IBM Watson for Oncology is one such app that has encountered this issue. An IBM document leaked showed that the AI system gave unsafe or wrong treatment suggestions on at least five occasions (Brown, 2018). According to Brown (2018) Watson's training technique, which involved doctors at the Memorial Sloan Kettering (MSK) Cancer Center synthesizing cancer cases instead of real patient data, was the root cause of this issue. Despite MSK's insistence that no mistakes were made during system testing or incorrect recommendations were given to real patients, the case highlights the issue of opaque training and decision-making in AI (Brown, 2018).

We should encourage the openness of AI systems to meet these challenges, which are undoubtedly relevant today. Apart from operational efficiency, transparency is a factor that can help build an equitable culture for patients of any color or income within healthcare systems (Ronen, 2024). Being able to align with general principles and specific goals for AI decision-making is crucial to the creation of trust and the preservation of the integrity of a healthcare system as increasingly it turns to the support of advanced technologies.

3.1.5. Algorithmic Bias in Healthcare: Challenges and Implications

The concern over whether the artificial intelligence (AI) platforms developed are biased or not has emerged and gained attention, particularly in the healthcare setting. This paper defines algorithmic bias as' systematic and repeatable errors in a computer system that create an 'unfair' outcome—the algorithm favoring one category over another in ways beyond its fundamental design' (Clifton, 2023; Wikipedia, 2023). Algorithmic bias is not just an ethical issue but also presents practical problems. While algorithmic bias can harm marginalized communities in domains such as banking, housing, and education, its impact is particularly concerning in healthcare, where it can exacerbate inequalities and compromise patient care (O'Neil, 2016).

Given the severity of this issue, the Biden administration issued an Executive Order mandating that "agencies shall consider opportunities to prevent and remedy discrimination, including by protecting the public from algorithmic discrimination" (House, 2023b). Healthcare widely uses algorithms for tasks like diagnosis, prognosis, therapy, risk assessment, resource allocation, and triage. However, biased algorithms have already caused harm; for instance, an algorithm that estimated kidney function based on race delayed organ transplants for Black patients, resulting in disproportionately favorable estimations for White patients (Vyas, 2020).

To mitigate these risks, it is crucial for AI developers to acknowledge and address biases at every stage of system development. This includes careful consideration when selecting machine learning (ML) technologies, designing algorithm training processes, and curating datasets. Recognizing ethnic, skin color, gender, age, and disability disparities is possible (Gerke, 2023). For instance, systematic errors in the prognostic models for breast cancer risk label Black patients as low-risk, despite well-documented performance disparities (Price, 2019). Similarly, algorithms trained on data from German hospitals may perform poorly in the U.S. context due to differences in demographics, treatment approaches, and medication regimens (Obermeyer, Powers, Vogeli, & Mullainathan, 2019).

AI biases can originate from the source data, the model architecture, the selection of metrics, or even from the post-deployment phase (Kerstin & Vokinger, 2021). For instance, the algorithms primarily train on data sets from White patients, which may not accurately represent the health needs and status of Black patients due to insufficient data collection from diverse sources (Gerke, 2023). Furthermore, disparities in healthcare accessibility and spending exacerbate these challenges, impacting the modeling and foresight of risks (Seyyed-Kalantari et al., 2021).

Reducing algorithmic bias in the health care industry is a complex issue that needs addressing in terms of algorithms and approaches to datasets, testing and protocols, and design. Only in this way can we support AI systems and present an opportunity to provide equitable, effective, and ethical healthcare solutions for large and different populations.

3.1.6. Cyber Security Challenges in the Integration of AI into Healthcare

Cyber security is undoubtedly one of the most profound and continuous issues with the integration of artificial intelligence (AI) into the healthcare system. These and similar healthcare services and products have become the 'platform of the Internet of Things' (IoT), exposing a significant portion of IoT infrastructure to cyber risk (Security, 2023). Criminal actors, non-state actors, and cybercriminal groups take advantage of these weaknesses to sabotage critical healthcare delivery, steal vital information, or meddle with financial processes (Security, 2023). These actors are upping their developments to either blackmail or disrupt crucial health care mechanisms, which is very dangerous for certain patients on an individual basis and for the consolidated health systems as a whole.

As Masons. (2017) explained, potential attacks can occur in diagnostic equipment, wearable devices, wireless tablets, and medical instruments used by the health care service. These attacks frequently jeopardize patient confidentiality and health by introducing harmful elements like viruses, Trojan horses, or worms, which can significantly compromise data security (Gerke et al., 2020). Moreover, the presence of slandered or distorted data as well as skewed algorithms may result in dangerous or improper treatment practices that compound threats (Gerke et al., 2019). AI-based technologies are susceptible to deception, as they may provide inaccurate patient information or alter health publications. For example, very slight changes in the value of inputs can lead to an AI system, such as a diagnostic one, predicting with almost complete certainty that a benign mole is malignant—this shows that such systems can make colossal errors (Gerke, 2023).

As some of the recent hackings, like the "WannaCry" ransomware attack of 2017, prove, these threats aren't fictitious. This attack through complex malware targeted the UK's National Health Service (NHS), stopped majority of FedEx services globally, and affected over 300,000 computers across 150 countries, including Russia, Taiwan, Ukraine, and India (Graham, 2017). Such cases underscore the necessity for better protective strategy to guard the healthcare system from such disruption in the future.

To address the aforementioned challenges, the European Union has implemented a variety of cyber security measures pertaining to key infrastructures and data. The EU has Directive on Security of Network and Information Systems (NIS) with mandatory procedures that include the EU member states being obligated to develop national cyber security strategies and designate operators of essential services (OES) in important sectors like healthcare, energy, transport, banking, etc (Commission, 2023a). Another regulation, the General Data Protection Regulation, reinforces this directive by mandating organizations to implement technical and organizational safeguards for personal data, thereby incorporating cyber security into data protection (Commission, 2023b).

Additionally, the EU Cyber security Act enhances the EU's cyber security posture by designating ENISA as a permanent entity and establishing a cyber-security certification scheme for products, services, and processes (Act, 2019). Other new laws, including the European Commission (2023) also seek to build up the EU's capabilities on detection, understanding of the operating environment, and response to the cyber threats (Union, 2023).

Federal and state legislation currently guides the development of cyber security regulations in the US. Federal laws embracing data security include the Health Insurance Portability and Accountability Act (HIPAA) for health information, the Gramm-Leach-Bliley Act for financial information, and the Federal Information Security Management Act (FISMA) for governmental information. These laws are specific to a single domain and lack the systematic and centrally facilitated approach observed in the EU.

These new developments in cyber security regulations in the EU and the USA are significant steps towards safeguarding the healthcare sector from cyber risks. However, computer security remains a global issue that requires collaborative efforts at the international level. To achieve the protected, secure, and ethical use of artificial intelligence in healthcare systems across the world, we must meet the mentioned challenges on the international level.

3.1.7. AI and Intellectual Property Rights in Healthcare

Artificial intelligence and data constitute the cornerstones of innovation and development across the health care industry. The rapid advancement of these technologies necessitates the implementation of effective and appropriate patent protection under IPR laws, which will safeguard algorithms, software, medical devices, and treatment plans. Nevertheless, there has been a lively debate concerning the patentability of certain AI-powered inventions, particularly in relation to the issue of inventor identity. The integration of AI in the creation of inventions raises essential questions about inventive credit and the deserved reward for AI innovations (Macedo, 2023). First of all, AI techniques mostly utilize

big data, for example, electronic health records, genomic data, and data from medical imaging. Control over this data has become a major matter of concern, with potential impacts that vary from patients' privacy to data protection and ownership of intangible assets (Cai, 2021). In the healthcare sector, companies invest heavily in developing patented AI technologies and algorithms, seeking to gain a competitive market advantage (GPF, 2024). Safeguarding trade secrets and proprietary data is essential for maintaining this edge, and businesses employ strategies such as encryption and nondisclosure agreements to prevent unauthorized access and misuse (Nicholson, 2016).

Despite the rapid evolution of AI technologies in healthcare, they present substantial challenges to intellectual property frameworks, particularly in the context of "black box" machines. Cyber security Solidarity Act. Protecting investments in "black box" algorithms is particularly complex due to the significant resources required for their development. Developers must acquire, assemble, or create the extensive datasets needed to train these algorithms, gather the expertise and materials for successful implementation, and verify the results to ensure accuracy. Intellectual property rights are presumed to provide some level of protection for these information commodities, encouraging businesses to invest in innovation without fear of misappropriation (Lemley, 2004).

However, IPR frameworks do not function seamlessly with "black box" medicine. Recent rulings by the U.S. Supreme Court have complicated the patenting of "black box" algorithms. In Mayo Collaborative Services v. Prometheus Laboratories (2012) the Court held that laws of nature cannot be patented. The decision invalidated a diagnostic test patent that adjusted a patient's prescription dosage by measuring metabolite levels in their blood. The Court ruled that "well-understood, routine, conventional activity previously engaged in by scientists in the field" does not transform an unpatentable law of nature into a patent-eligible application (Eisenberg, 2015; Price, 2017). This interpretation of Section 101 of the Patent Act has created significant hurdles for patenting AI-driven diagnostic tools and treatments.

The collaboration between healthcare companies and AI technology suppliers further complicates IPR considerations. Joint ventures, research alliances, and licensing agreements are common, with parties exchanging licenses for patented technologies and access to confidential data. Negotiating favorable terms in these agreements is crucial for maximizing the value of AI advancements and fostering ongoing innovation in healthcare (Macedo, 2023; Walsh, 2022). Stakeholders in AI-based healthcare technologies are likely to disagree over copyright ownership, leading to legal disputes such as contract breaches, theft of trade secrets, and patent infringement. These cases can determine Ownership and Commercialization Rights which define industry standards and norms (Nagarathna, 2022).

The governance of AI in a setting is constantly shifting and changing, posing a challenge for organizations to maintain compliance and enforce the proper legal disposition of intellectual property rights. The regulatory authorities must balance the risk of stifling innovation with their efforts to promote safe, effective, and ethical solutions. Due to IPR, regulations relating to the development, testing, and sale of AI systems are significant and continue to evolve.

Allowing AI into the field of IP in healthcare is a delicate area that affects healthcare innovation, regulation, cooperation, and protection systems. The stakeholders must manage these challenges, defend IPR, and ensure patient-relevant and societal benefits from innovation in order to fully realize the benefits of various AI technologies (IBM, 2023; Nagarathna, 2022).

4. CONCLUSION

This work centers on AI's interaction with the healthcare sector, highlighting a plethora of evolving ethical and legal issues that demand immediate attention. While AI technologies hold great promise, permeating nearly every aspect of healthcare organizations, their implementation necessitates a focus on controlling patient benefits and enhancing health outcomes while adhering to ethical norms.

Three of the most important ethical questions arising from the use of Artificial Intelligence in the delivery of health care include consent, data privacy, and data security. AI systems depend on large amounts of highly confidential patient data to draw patterns and make predictions about possible outcomes and are thus inherently vulnerable to hackers, data breaches, and the general misuse of individuals' PHIs. To mitigate these risks, it is crucial to implement robust data protection measures, enforce strict access control, and adhere to data protection legislation such as the GDPR in the EU and the HIPAA in the USA. These measures are important for the protection of patients' data and building trust among people in AI healthcare solutions.

Additionally, measuring bias, equity, and justice in algorithms poses significant risks in the healthcare sector. Social imbalances are the root cause of most AI-applied problems, and if we reinforce these through biases in training data, algorithm design, or unfair interpretation of results, we risk perpetuating the existing inequality in healthcare and treatment access. For instance, skewed training datasets often lead to skewed algorithms that negatively impact marginalized groups. Solving these problems must involve diverse datasets, improving a fair evaluation of algorithms, and integrating accountability and transparency into device applications.

These issues demonstrate that coordination with policymakers, medical practitioners, technologists, and ethicists is inevitable. Rapid delivery of these structures and formulations necessitates a multidisciplinary approach that simultaneously generates ethical frameworks, provides regulatory oversight of AI technologies, and ensures their widespread respect and trust. In order to mitigate these biases and enhance healthcare equity, we need to focus more on diversifying the data sources, enhancing the fairness of the algorithms internally, and fostering greater understanding of their functioning.

Therefore, the role of AI in healthcare is revolutionary as it opens up new avenues for the development of medical technologies and provides the population with improved health care services. Most importantly, stakeholders can use the possibilities offered by AI technologies in full measure, eliminating the ethical and legal risks or managing them effectively. We must also protect the ethical, equal, and just foundations of health care, which will require ongoing cooperation from scholars. Together, these activities will establish the foundation for the continued advancement of AI in healthcare, which will positively influence the statistics of effective healthcare and benefit society.

Funding:
This study received no specific financial support.

Institutional Review Board Statement:
Not applicable.

Transparency:
The authors state that the manuscript is honest, truthful, and transparent, that no key aspects of the investigation have been omitted, and that any differences from the study as planned have been clarified. This study followed all writing ethics.

Competing Interests:
The authors declare that they have no competing interests.

Authors' Contributions:
All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

REFERENCES

Act, T. E. (2019). *Shaping Europe's digital future*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Brown, J. (2018). *BM watson reportedly recommended cancer treatments that were 'unsafe and incorrect*. Retrieved from https://gizmodo.com/ibm-watson-reportedly-recommended-cancer-treatments-tha-1827868882

Cai, D. X. (2021). Privacy protection and secondary use of health data: Strategies and methods. *Biomed Res Int*, 6967166. https://doi.org/10.1155/2021/6967166

Calo, M. R. (2011). *The boundaries of privacy harm*. Retrieved from https://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf

Catherine Bushen, A. P. (2023). *Regulating AI in healthcare: Fall 2023 observations — Part one*. Retrieved from https://infermedica.com/blog/articles/regulating-ai-in-healthcare-fall-2023-observations-part-one

Clifton, J. Y. (2023). An adversarial training framework for mitigating algorithmic biases in clinical machine learning. *Digital Medicine, 6*(55), 1-10.

Cohen, I. G. (2018). *HIPAA and protecting health information in the 21st century*. Retrieved from https://jamanetwork.com/journals/jama/fullarticle/2682916

Commission, E. (2023a). *Data protection rules for the protection of personal data inside and outside the EU*. Retrieved from https://commission.europa.eu/law/law-topic/data-protection_en

Commission, E. (2023b). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Conversation, T. (2023). *How the UK is getting AI regulation right*. Retrieved from https://theconversation.com/how-the-uk-is-getting-ai-regulation-right-206701

Eisenberg, R. S. (2015). Diagnostics need not apply. *University of Michigan Law School University of Michigan Law School Scholarship Repository, 21*(2), 256-286.

European Commission. (2023). *Proposal for a regulation of the European parliament and of the council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. EUR-Lex*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0209

European Union. (2016). *General data protection regulation (GDPR): Regulation (EU) 2016/679 of the European parliament and of the council of 27 april 2016. official journal of the European Union, L*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Farooqui, M. O., Sharma, B., & Gupta, D. (2022). Inheritance of digital assets: Analyzing the concept of digital inheritance on social media platforms. *Novum Jus, 16*(3), 413–435. https://doi.org/10.14718/NovumJus.2022.16.3.15

Gerke, S. (2023). Ethical and legal issues in artificial intelligence-based cardiology. In A. C. Chang & A. Limon (Eds.), Intelligence-Based Cardiology and Cardiac Surgery: Artificial Intelligence and Human Cognition in Cardiovascular Medicine. In (pp. 415–419): Academic Press. https://doi.org/10.1016/B978-0-323-90534-3.00034-2.

Gerke, S., Minssen, T., & Cohen, I. G. (2019). Ethical and legal issues of ingestible electronic sensors. *Nature Electronics, 2*(8), 329–334. https://doi.org/10.1038/s41928-019-0298-6

Gerke, S., Minssen, T., & Cohen, I. G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In A. Bohr & K. Memarzadeh (Eds.), Artificial intelligence in healthcare. In (pp. 295–336): Elsevier. https://doi.org/10.1016/B978-0-12-818438-7.00012-5.

GPF. (2024). *Impact of pharmaceutical patent on healthcare sector in India*. Retrieved from https://www.globalpatentfiling.com/blog/Impact-of-Pharmaceutical-Patent-on-Healthcare-Sector-in-India#:~:text=The%20advent%20of%20product%20patents,necessary%2C%20life%2Dsaving%20drugs

Graham, C. (2017). *NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history*. Retrieved from https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/#:~:text=Download%20our%20app-,NHS%20cyber%20attack%3A%20Everything%20you%20need%20to%20know%20about,biggest%20ransomware'%20offensive%20in%20hi

Gupta, P. D. (2023). Data privacy in healthcare: In the era of artificial intelligence. *Indian Dermatology Online Journal, 53*(23), 788-792.

House, T. W. (2023a). *Executive order on further advancing racial equity and support for underserved communities through the federal government*. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive-order-on-further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/

House, T. W. (2023b). *FACT SHEET: President biden issues executive order on safe, secure, and trustworthy artificial intelligence*. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

IBM. (2023). *The benefits of AI in healthcare*. Retrieved from https://www.ibm.com/blog/the-benefits-of-ai-in-healthcare/

Kerstin, N., & Vokinger, S. F. (2021). Mitigating bias in machine learning for medicine. *Communications Medicine, 1*(25), 1-3.

Krishnan Ganapathy, M. N. (2021). Artificial intelligence and healthcare regulatory and legal concerns. *Telehealth and Medicine Today, 6*(2), 1-15. https://doi.org/10.30953/tmt.v6.252

Labhaoise, N., & Fhaoláin, A. H. (2020). *Assessing the appetite for trustworthiness and the regulation of artificial intelligence in Europe*. Retrieved from https://ceur-ws.org/Vol-2771/AICS2020_paper_53.pdf

Lemley, M. A. (2004). Ex ante versus ex post justifications for intellectual property. *The University of Chicago Law Review, 71*(29), 129-149.

Lyons, E. F. (2016). *The administration's report on the future of artificial intelligence*. Retrieved from https://obamawhitehouse.archives.gov/blog/2016/10/12/administrations-report-future-artificial-intelligence

Macedo, R. C. (2023). *Obstacles to healthcare AI: Legal issues relating to the increasing use of AI in healthcare and medical technologies*. Retrieved from https://www.ibanet.org/Obstacles-healthcare-ai

Markose, R. K. A. (2016). Medical ethics. *Journal of Pharmacy and Bioallied Sciences, 8*(S1), S1–S4. https://doi.org/10.4103/0975-7406.191934

Masons., P. (2017). *New 'digital' pills pose data protection and cybersecurity challenges for drugs manufacturers and health bodies, says expert*. Retrieved from https://www.pinsentmasons.com/out-law/news/new-digital-pills-pose-data-protection-and-cybersecurity-

challenges-for-drugs-manufacturers-and-health-bodies-says-expert
Mayo Collaborative Services v. Prometheus Laboratories, I. (2012). *566 U.S. 66. Supreme court of the United States*. Retrieved from https://supreme.justia.com/cases/federal/us/566/66/
Moore, S. (2023). *Ethical considerations in AI-Driven healthcare*. Retrieved from https://www.news-medical.net/health/Ethical-Considerations-in-AI-Driven-Healthcare.aspx#5
Nagarathna, P. K. M. (2022). *Cyber security in healthcare with artificial intelligence*. Retrieved from https://ieeexplore.ieee.org/document/9972597/metrics#metrics
Naik, N., Hameed, B. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., . . . Smriti, K. (2022). Legal and ethical consideration in artificial intelligence in healthcare: Who takes responsibility? *Frontiers in Surgery, 9*, 862322. https://doi.org/10.3389/fsurg.2022.862322
Nicholson, R. A. (2016). Privacy and accountability in black-box medicine. *Michigan Telecommunication and Technology Law Review, 23*(1), 1-43.
O'Neil, C. (2016). *Weapons of math destruction how big data increases inequality and threatens democracy*. New York: Crown.
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. https://doi.org/10.1126/science.aax2342
Parliament, E. (2023). *EU AI act: First regulation on artificial intelligence*. Retrieved from https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
Price, W. N. (2019). Medicial AI and contectual bias. *Harvard Journal of Law & Technology, 33*(1), 65-116.
Price, W. N. I. I. (2017). Artificial intelligence in health care: Applications and legal implications. *Michigan Telecommunications and Technology Law Review, 23*(1), 1–43.
Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. (2017). Writ Petition (Civil) No. 494 of 2012. Supreme Court of India. Reported in (2017) 10 SCC 1; AIR 2017 SC 4161.
Reuters. (2024). *U.S supreme court chief justice urges caution as ai reshapes legal field*. Retrieved from https://www.thehindu.com/news/international/us-supreme-court-chief-justice-urges-caution-as-ai-reshapes-legal-field/article67695726.ece
Ronen, O. (2024). *Transparent ai in healthcare: Transforming the industry for the better*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2023/12/05/transparent-ai-in-healthcare-transforming-the-industry-for-the-better/?sh=3da282217d26
Security, U. D. (2023). *Cybersecurity*. Retrieved from https://www.dhs.gov/topics/cybersecurity
Seyyed-Kalantari, L., Zhang, H., McDermott, M. B., Chen, I. Y., & Ghassemi, M. (2021). Underdiagnosis bias of artificial intelligence algorithms applied to chest radiographs in under-served patient populations. *Nature Medicine, 27*(12), 2176-2182. https://doi.org/10.1038/s41591-021-01595-0
Tech, I. G. (2020). *AI Update: White house issues 10 principles for artificial intelligence regulation*. Retrieved from https://www.insideglobaltech.com/2020/01/14/ai-update-white-house-issues-10-principles-for-artificial-intelligence-regulation/
Union, E. C. (2023). *Cyber solidarity act: Member states agree common position to strengthen cyber security capacities in the EU*. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2023/12/20/cyber-solidarity-act-member-states-agree-common-position-to-strengthen-cyber-security-capacities-in-the-eu/
UNT. (2021). *The national security commission on artificial intelligence*. Retrieved from https://cybercemetery.unt.edu/nscai/20211005220330/https://www.nscai.gov/
Vincent, J. (2024). *AI that detects cardiac arrests during emergency calls will be tested across Europe this summer*. Retrieved from https://www.theverge.com/2018/4/25/17278994/ai-cardiac-arrest-corti-emergency-call-response
Vyas, D. A. E. L. (2020). Hidden in plain sight — reconsidering the use of race correction in clinical algorithms. *PSNet, 383*(9), 874-882.
Walsh, A. G. (2022). *Artificial intelligence is breaking patent law*. Retrieved from https://www.nature.com/articles/d41586-022-01391-x
Wikipedia. (2023). *Algorithmic bias*. Retrieved from https://en.wikipedia.org/wiki/Algorithmic_bias
Wolford, B. (2020). *What is GDPR, the EU's new data protection law?* Retrieved from https://gdpr.eu/what-is-gdpr/