Data protection and AI compliance in health research: a relevant resource for institutions and companies against algorithmic vulnerability

*Giuseppe Claudio Cicu, Riccardo Michele Colangelo, Luca Saba**

DATA PROTECTION AND AI COMPLIANCE IN HEALTH RESEARCH: A RELEVANT RESOURCE FOR INSTITUTIONS AND COMPANIES AGAINST ALGORITHMIC VULNERABILITY

ABSTRACT: Artificial intelligence (AI) is becoming integral to health research, with applications in diagnosis, prognosis, and imaging segmentation across several medical fields. However, integrating health, biometric, and genetic data into AI systems raises ethical, legal, and practical challenges, particularly concerning discrimination and bias. Studies highlight the presence of bias, hindering AI model development in healthcare. Compliance with current legislation (e.g., GDPR), international frameworks (e.g., ISO), and forthcoming European AI regulation is pivotal. This paper emphasizes integrating these requirements into public entities and private organizations to ensure fair AI development and utilization in the health sector.

KEYWORDS: AI Act; GDPR; Compliance; Health Data; Algorithmic vulnerability.

ABSTRACT: L'intelligenza artificiale (AI) sta diventando parte integrante della ricerca sanitaria, con applicazioni nella diagnosi, nella prognosi e nella segmentazione delle immagini in diversi campi medici. Tuttavia, l'integrazione di dati sanitari, biometrici e genetici nei sistemi di IA solleva sfide etiche e giuridiche, in particolare per quanto riguarda *bias* e discriminazione. Diversi studi evidenziano la presenza di bias, che ostacolano lo sviluppo e l'impiego di modelli di IA nel settore sanitario. La conformità alla legislazione vigente (ad esempio, GDPR), agli standard internazionali (ad esempio, ISO) e alla normativa europea sull'IA è fondamentale. Questo articolo vuole sottolineare la necessità di una corretta implementazione di questi requisiti negli enti pubblici e nelle organizzazioni private per garantire uno sviluppo e un utilizzo corretto dell'IA nel settore sanitario.

PAROLE CHIAVE: AI Act; GDPR; Compliance; Dati sanitari; Vulnerabilità algoritmica.

* *Giuseppe Claudio Cicu: Ph.D. Student, University of Turin. Mail: giuseppeclaudio.cicu@unito.it; Riccardo Michele Colangelo: Ph.D. Student, Universitas Mercatorum, Rome. Mail: riccardomichele.colangelo@studenti.unimercatorum.it; Luca Saba, Full Professor of Diagnostic Imaging and Radiotherapy, University of Cagliari. Mail: lucasaba@unica.it. Giuseppe Claudio Cicu is author of paragraphs 2.1, 3, 3.1, 5, 7; Riccardo Michele Colangelo is author of paragraphs 2.2, 3, 3.2, 5, 7; and Luca Saba is author of paragraphs 1, 3, 4, 5, 6. The article was subject to a double-blind peer review process.*

ISSN 2284-4503

SOMMARIO: 1. Introduction – 2. The regulatory background – 3. Voluntary frameworks and technical standards – 4. AI and bias in medical research – 5. Compliance and mitigation strategies – 6. Bridging the gap: from regulation to practice – 7. Conclusions.

1. Introduction

The advent and proliferation of Artificial Intelligence (AI) in the medical sector marks a pivotal transition in healthcare delivery and medical research[1]. AI's unparalleled ability to analyze vast datasets has unlocked innovative avenues for enhancing diagnostic accuracy, tailoring patient care, and streamlining healthcare workflows. These advancements are not only pivotal in managing complex diseases but also in predicting patient outcomes, thereby revolutionizing the landscape of medical care and research.

A quintessential example of AI's impact can be observed in the field of cardiovascular diseases, the leading cause of global morbidity and mortality[2]. Recent integrations of AI technologies in cardiovascular medicine have demonstrated promising results, ranging from improved diagnostic precision to nuanced patient risk assessments. By leveraging complex algorithms and machine learning models, researchers and clinicians are now better equipped to decode the intricate patterns of cardiovascular diseases, facilitating early detection and intervention.

However, as AI systems become more ingrained in healthcare processes, a spectrum of legal and ethical challenges emerges, particularly concerning data protection, privacy, and the potential for algorithmic bias[3]. The integration of health, biometric, and genetic data into AI systems raises substantial concerns about the safeguarding of fundamental rights. These concerns are exacerbated by evidence of varying AI algorithm performances across different racial and ethnic groups, which can lead to discrimination and bias, undermining the equity and fairness of healthcare services.

As AI continues to redefine the horizons of medical research and healthcare delivery, it is imperative to address these challenges head-on. Ensuring compliance with data protection laws, such as the General Data Protection Regulation (GDPR), adhering to international frameworks and technical standards along with the forthcoming European regulation on AI as well as statements by the competent supervisory authorities (e.g. the Decalogue of the Italian Data Protection Authority regarding health services and AI) is crucial. This paper aims to explore the legal and ethical considerations surrounding the use of AI in healthcare, with a particular focus on mitigating algorithmic bias and enhancing data protection. By exploring these dimensions, we strive to pave the way for a more equitable and responsible integration of AI technologies in the health sector, safeguarding the rights and well-being of individuals across diverse racial and ethnic backgrounds.

[1] M. MOOR, O. BANERJEE, Z. S. H. ABAD, H. M. KRUMHOLZ, J. LESKOVEC, E. J. TOPOL, P. RAJPURKAR, *Foundation models for generalist medical artificial intelligence*, in *Nature*, 616, 7956, 2023, 259–265.

[2] R. CAU, F. PISU, A. PINTUS, V. PALMISANO, R. MONTISCI, J. S. SURI, R. SALGADO, L. SABA, *Cine-cardiac magnetic resonance to distinguish between ischemic and non-ischemic cardiomyopathies: a machine learning approach*, in *European Radiology,* 34, 2024, 5691-5704.

[3] R. VANDERSLUIS, J. SAVULESCU, *The selective deployment of AI in healthcare: An ethical algorithm for algorithms*, in *Bioethics*, 38, 5, 2024, 391–400.

2. The regulatory background

The integration of AI into healthcare not only promises to enhance medical research and patient care but, at the same time, also necessitates a rigorous legal and regulatory framework to address the myriad challenges it presents. This section provides an overview of the key laws, regulations, and standards governing data protection and AI in healthcare, emphasizing the importance of these frameworks in ensuring the ethical and secure use of AI technologies.

2.1. The European Artificial Intelligence Act

The spread of AI systems raises significant legal and ethical concerns, including issues related to privacy, transparency, accountability, discrimination, and bias. Consequently, the development and deployment of AI technologies require the implementation of appropriate legal rules to ensure trustworthy, accountable, and non-discriminatory access and utilization of such systems, especially when sensitive data categories such as health, genetic, and biometric data are involved[4].

These concerns have led the European Union to adopt a uniform legal framework that establishes harmonized rules on AI, aimed at improving the functioning of the internal market and promoting the uptake of human-centric and trustworthy AI, while ensuring a high level of protection for health, safety, and fundamental rights (the "EU AI Act")[5].

The subjective and objective scope of the regulation's content suggest that the European Union has also sought to achieve the so-called Brussels effect in relation to artificial intelligence. This term refers to the EU's ability to establish its legislation as a global standard within the international regulatory framework[6].

The EU AI Act introduces a risk-based classification of AI systems, aiming to balance technological innovation with the safeguarding of fundamental rights. Specifically, it categorizes AI applications into four risk levels: unacceptable risk, high risk, limited risk, and minimal risk.

AI systems that pose a clear threat to safety, livelihoods, or rights fall into the "unacceptable risk" category and are banned outright[7]. Examples of such systems include social scoring by governments and real-time biometric identification in public spaces.

"High risk" systems are subject to strict requirements and include applications in critical infrastructure, education, employment, essential private and public services, law enforcement, migration, and border control. The EU AI Act mandates rigorous testing procedures, documentation, compliance,

[4] *Study on Health Data, Digital Health and Artificial Intelligence in Healthcare*, Directorate-General for Health and Food Safety, European Commission, 16.

[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending regulations (EC) no 300/2008, (EU) no 167/2013, (EU) no 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and directives 2014/90/EU, (eu) 2016/797 and (EU) 2020/1828.

[6] B. Anu, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020).

[7] See Art. 5, EU AI Act.

and risk and quality management measures to ensure these systems are transparent, secure, and fair[8].

AI applications characterized by "limited risk" require specific transparency obligations. For instance, users must be informed when they are interacting with an AI system, allowing them to make informed decisions[9].

Several AI systems fall into the category of "minimal risk" and are subject to few legal requirements. Examples include AI-enabled video games and spam filters.

Under this risk-based approach, most AI applications adopted in the healthcare field fall into the high-risk category, reflecting the need to ensure high standards of patient safety, transparency, accountability, data privacy, and ethical standards.

Article 6.1 of the EU AI Act states that an AI system is classified as high-risk if it meets both of the following criteria, regardless of whether it is marketed or utilized independently of the products mentioned in points (a) and (b): «(a) The AI system is intended to be used as a safety component of a product, or it is a product itself, as specified by the Union harmonization legislation listed in Annex I. (b) The product, either the one whose safety component is the AI system mentioned in point (a) or the AI system itself as a product, must undergo a third-party conformity assessment before it can be marketed or put into service, in accordance with the Union harmonization legislation listed in Annex I».

With reference to the first condition, Annex I explicitly refer to Regulation (EU) 2017/745 ("MDR") related to medical devices. Regarding the second condition, Annex VIII, Chapter III, Rule 11 of the MDR (labeled "Classification") provides that software intended to provide information used to make decisions for diagnostic or therapeutic purposes is classified as class IIa, except if such decisions have an impact that may cause death or an irreversible deterioration of a person's state of health, in which case it is in class III; or a serious deterioration of a person's state of health or a surgical intervention, in which case it is classified as class IIb.

Software intended to monitor physiological processes is classified as class IIa, except if it is intended for monitoring vital physiological parameters, where the nature of variations in those parameters is such that it could result in immediate danger to the patient, in which case it is classified as class IIb.

Under these premises, such software often requires a third-party conformity assessment before it can be marketed or put into service. Thus, they fall within the application of the EU AI Act as high-risk systems when related to AI systems.

With reference to the health research activities, the EU AI ACT provides specific exclusions and instruments aimed at assuring that scientific research activities on AI systems are not undermined by the Regulation. Such provisions are without prejudice to the obligation to comply with this Regulation where an AI system falling within the scope of this Regulation is placed on the market or put into service as a result of such research and development activity and to the application of provisions on AI regulatory sandboxes and testing in real world conditions[10].

[8] See Art. 5, EU AI Act.

[9] See Art. 50, EU AI Act.

[10] See Whereas n. 25, EU AI Act.

In this regard, the main exclusion regarding the research activities – therefore applicable to the health research sector - is set out in Art. 2.6. of AI EU ACT, which states that the EU AI ACT does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research[11].
Moreover, the Regulation also provides that its provisions do not apply to any research regarding AI systems or AI models prior to their being placed on the market or put into service, with the exclusion of testing in real world conditions[12].
Finally, in order to facilitate the involvement of relevant actors within the AI ecosystems, such as research and experimentation labs and individual researchers, the EU AI ACT provides the so called "AI regulatory sandboxes": controlled environments where innovative AI systems can be developed, trained, tested and validated for a limited time before their being placed on the market or put into service[13].

2.2 Data Protection and AI in the health research sector

The considerations set out regarding the EU AI Act must be enriched by a synthetic insight of some relevant data protection issues. All this, with the awareness that the rules of this Regulation neither solve specific problems nor fill gaps in the data protection regulatory framework, even though they apply to multiple sectors, including healthcare and health research[14].
With particular regard to the EU Regulation 2016/679 (General Data Protection Regulation), it is first of all necessary to highlight numerous references to the GDPR laid down in the EU AI Act: significantly, the number of such references increased during the AI Regulation approval[15].
This entails the need to consider both disciplines, in cases of any personal data processing carried out by automated means, among which AI systems are included in whole or in part.
This is all the truer with regard to the (AI) processing of special categories of personal data[16]: data, therefore, that can reveal data subject's vulnerabilities and expose him to discriminatory conducts.
This brief introduction underlines the importance of a reasoned and clear identification of the legal basis of the specific processing, since pursuant to art. 9, paragraph 1 GDPR the processing of special categories of personal data «shall be prohibited», unless there is (at least) one of the legal bases indicated in paragraph 2 of the same article.

[11] See Art. 2.6., EU AI Act.

[12] See Art. 2.9., EU AI Act.

[13] See Art. 57, EU AI Act.

[14] Cfr. P. Falletta, A. Marsano, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Rivista italiana di informatica e diritto*, 1, 2024, 123.

[15] 30 references to EU Regulation 2016/679 are included in the final text of the EU AI Act.

[16] According to art. 9, par. 1 GDPR, special categories of personal data are «personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation».

Here we can find not only the explicit consent given by the data subject (mandatory, for instance, for personal data processing made by healthcare apps[17]), but also the aim to protect the vital interests of the data subject. A processing of special categories of personal data can be considered lawful also when it «is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services» or «for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices».

Regarding the health field, in 2023 the Italian Data Protection Authority (IDPA) set a Decalogue for the implementation of national health services through Artificial Intelligence[18] focusing, for instance, on the processing legal basis, the roles of natural or legal person involved in the specific processing and the importance of the privacy by design and by default principles. In this Decalogue, the IDPA[19] clarifies and sets out the principles of knowledge, not exclusivity and not algorithmic discrimination, considered as «three cardinal principles that must govern the use of algorithms and AI tools in the execution of relevant public interest».

The principle of knowledge regards «the right to know the existence of decision-making processes based on automated processing and, in this way, case, to receive significant information about the logic used, so as to be able to understand», while the principle of non-exclusivity of the algorithmic decision states that is necessary «in decision-making a human intervention capable of check, validate or deny the automatic decision» (c.d. human in the loop). Last but not least, we can find the crucial principle of algorithmic non-discrimination, meaning that «the data controller uses reliable AI systems that reduce opacity, the errors due to technological and/or human action, periodically checking efficiency also in the light of the rapid evolution of the technologies used, the appropriate mathematical or statistical procedures for profiling, setting out appropriate technical and organisational measures. This, including in order to ensure, the factors leading to inaccuracies in the data are corrected and minimised the risk of error, having regard to the potential discriminatory effects that inaccurate health data may determine against people (cf. recital 71 of the Regulation)».

The same Decalogue also states that, by means of interpretation, the GDPR requires that, in these cases of health data processing by AI, the information provided in compliance with the elements referred to in art. 13 and 14 of GDPR are not sufficient: data controllers have to highlight also “whether the processing is carried out in the learning phase of the algorithm (testing and validation) or in the next phase of application of the same, in the field of health services, representing data processing logics and characteristics; whether there are any obligations and responsibilities of health profession-

[17] R.M. COLANGELO, *App mediche e protezione dei dati personali. Alcuni spunti giuridici tra GDPR, codice privacy novellato e chiarimenti del Garante*, in *Autonomie locali e servizi sociali*, 2, 2019, 275-288.

[18] This Decalogue (in italian: *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale)* can be read on the Italian Data Protection Authority official website: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9938038.

[19] *Ibidem*, par. 4 (author's translation).

als, to which the data subject is addressed, to use health services based on AI; the diagnostic and therapeutic benefits of using such new technologies"[20].

This insight confirms the primary role of the data protection regulation to prevent any form of discrimination related to AI systems, particularly in the health sector, not only before the full applicability of the EU AI Act, but also when the recent European Regulation wasn't in force. These considerations are particularly relevant in the context of scientific research, especially with reference to health research, highlighting how the transparency requirements for data subjects, based on the GDPR, must now be integrated - both in the public sector and by enterprises - with specific references to the artificial intelligence systems employed, as well as the stage of the lifecycle of such systems in which the personal data processing for health research purposes takes place.

In completion of these arguments, the healthcare sector, and particularly health research, is also subject, from a *de iure condendo* perspective, to the Italian "disegno di legge" n. 1146, titled Provisions and delegation to the Government on Artificial Intelligence.

Article 7 of the disegno di legge n. 1146 addresses the use of artificial intelligence in healthcare and disability, prohibiting discrimination (paragraphs 1 and 2) and establishing the «right of individuals to be informed about the use of artificial intelligence technologies and the benefits, in terms of diagnostics and therapy, resulting from the use of new technologies, as well as to receive information on the decision-making logic employed». It also highlights the supportive role of such systems (paragraph 5) and the necessity for their reliability, requiring that these systems be «periodically verified and updated to minimize the risk of errors» (paragraph 6).

Even more relevant in this context is Article 8, regarding Research and Scientific Experimentation in the Development of Artificial Intelligence Systems in Healthcare. This article establishes that «data processing, including personal data, carried out by public and private entities for non-profit purposes in research and scientific experimentation in the development of artificial intelligence systems» in healthcare (for the purposes of disease prevention, diagnosis, treatment, drug development", and other specific objectives) «are declared of significant public interest in accordance with Article 32 of the Constitution and in compliance with Article 9, paragraph 2, letter g), of Regulation (EU) 2016/679 of the European Parliament and the Council, of April 27, 2016». Consequently, the legal basis for such processing is established by law where processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. This implies, as a general rule, that, if the law is approved without amendments, consent will not be required in health research conducted by private entities too.

The following paragraph also authorizes, «without further consent from the data subject where initially required by law, the secondary use of personal data devoid of direct identifiers, including data belonging to the categories referred to in Article 9 of Regulation (EU) 2016/679, by the entities referred to in paragraph 1».

The specific data processing, as outlined in paragraphs 1 and 2, must, however, be approved by the competent ethics committees and communicated to the Italian Data Protection Authority with specific formal requirements. Following this communication, «processing may begin thirty days after the

[20] *Ibidem,* par. 8 (author's translation).

aforementioned communication unless blocked by a decision from the Data Protection Authority» (paragraph 3).
Another fundamental aspect that involves a partial overlap between data protection and AI legislation is related to the exercise of the rights of the data subject enshrined in the GDPR.
In particular, art. 22, par. 1, GDPR[21], regarding automated individual decision-making processes, including profiling, provides that «the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her». In the following paragraph some exceptions are mentioned but is fundamental to underline that paragraph 3 states the implementation of «suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision». Art. 22, par. 4, GDPR also specifies the instances where automated decisions based on special categories of personal data could be legal: in these circumstances, «suitable measures to safeguard the data subject's rights and freedoms and legitimate interests» should be taken.

3. Voluntary frameworks and technical standards

Beyond formal regulations, international voluntary frameworks play a crucial role in guiding the responsible use of AI in healthcare. Initiatives like OECD's Principles on AI and the G20's AI Guidelines advocate for principles such as inclusivity, transparency, and accountability[22]. Other interesting voluntary frameworks to ensure a lawful and ethical implementation of AI systems are the ISO technical standard and the AI Pact, which will be described in the following paragraphs 3.1 e 3.2.

3.1. Some considerations regarding ISO applicable to the AI field

The International Organization for Standardization (ISO) plays a key role in shaping the use of AI in healthcare through the development of voluntary international standards. These standards cover various aspects of AI, partly aligned with the provisions of the EU AI Act, including data quality, security, and interoperability, providing guidelines for the ethical and effective implementation of AI technologies. Particularly, ISO/IEC 42001 provides technical standards such as (i) logging and record-keeping as one of the optional controls to consider for implementing risk treatment options, (ii) transparency, with a focus on providing information to users, and (iii) quality management systems, as a high-level standard. Other relevant international standards include ISO/IEC 23894 on AI Risk Management, ISO/IEC 5259, which describes a data quality model for data analytics and AI based on machine

[21] The specific right under art. 22 GDPR is considered better suited to protect the rights of natural persons, while there are no similar effective redress mechanisms in the EU AI Act: cf. O. Pollicino, G. De Gregorio, *Intelligenza artificiale, data protection e responsabilità*, in A. Pajno, F. Donati, A. Perrucci (eds.), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, 355.
[22] M. Rotenberg, *Human Rights Alignment: The Challenge Ahead for AI Lawmakers. In Introduction to Digital Humanism*, Cham, 2024, 611–622.

ISSN 2284-4503

learning, and the ISO/IEC 24029 series that provides robustness metrics for supervised classification/ regression models using statistical and empirical approaches[23].
Following such standards, corporate organizations and public bodies may anticipate implementing technical and ethical measures for AI adoption also in the health sector and in the medical research field. However, it should be noted that most of the mentioned international standards do not guarantee - or guarantee only partially - compliance with the provisions of the EU AI Act.

3.2. The EU AI Pact

In addition to the aforementioned technical standards, it is necessary to consider how the European Commission intends to promote and anticipate an effective and appropriate compliance with the EU AI Act, which, as has been stated, aims to avoid as much as possible violations of the fundamental rights of the persons involved and any discrimination on the basis of any erroneous bias by AI systems.
In this regard, the EU AI Act regulates the role of the European AI Office, already established from 24 January 2024 within the European Commission, which is responsible for «contributing to the implementation, monitoring and supervision of AI systems and AI models for general purposes, and AI governance»[24]. This Office now promotes the AI Pact[25], which is a recent initiative of the European Union, and more precisely of the European Commission, that intends to stimulate - also in this case at a completely voluntary level - the proactive adherence to the new discipline on AI, especially before it comes into force[26]. In short, this initiative underlines the importance of considering the AI legislation now in force, although not yet applicable and fully binding, encouraging the adherence to the principles established in it even before (and in view) the full applicability of the EU AI Act as a whole.
The AI Pact is directly aimed at organizations, enterprises and companies - which can be involved in the processing of health data both as data controllers and as data processors - and underlines the growing importance of the development and correct use of AI systems also in the context of business activities, in order to protect individuals (and data subjects) in conditions of vulnerability and therefore to prevent any algorithmic discrimination.
The AI Pact is based on two pillars: the collection and exchange of best practices and information on the EU AI Act implementation process in the specific fields of the AI Pact network, as well as facilitating the commitments of enterprises and companies, so as to encourage both providers and deployers to prepare in time, taking the necessary measures and actions towards (future) compliance with the European framework on AI and its requirements and obligations.
This approach, which highlights one of the shortcomings of a regulation that is likely to be old[27]. It is still agreeable, as it helps to consider how it is not possible - as it was not before the final approval of

[23] For a comprehensive examination of the operational areas of ISO with reference to artificial intelligence, see *Analysis of the preliminary AI standardisation work plan in support of the AI Act*, JRC Technical Report, European Commission, 2023.
[24] Art. 3, par. 1, n. 4, EU AI Act.
[25] Available at: https://digital-strategy.ec.europa.eu/en/policies/ai-pact.
[26] The European Commission, through its Office, is «seeking the industry's voluntary commitment to anticipate the AI Act and to start implementing its requirements ahead of the legal deadline» (ibidem).

the EU AI Act - to say that the development and use of AI systems is completely free from any regulatory constraint. This is particularly true in the context of health-related data processing implemented through AI systems, regardless of the purposes of the processing and the public or private nature of the data processor or data controller.

4. AI and bias in medical research

For the purpose of this paper, we will focus on the cardiovascular field that represents the first cause of death worldwide[28]. The integration of AI in cardiovascular medicine has been marked by both significant achievements and challenges, particularly concerning biases that impact diagnostic accuracy across different racial and ethnic groups.

4.1. Successes in cardiovascular medicine

One of the most notable successes of AI in cardiovascular medicine is its ability to enhance diagnostic precision. For instance, deep learning models have been employed to interpret magnetic resonance, significantly improving the detection of pathologies[29]. These models analyze patterns in Magnetic Resonance images with a level of detail and accuracy that surpasses conventional methods, leading to earlier and more accurate diagnoses. AI algorithms have also been instrumental in developing predictive models for cardiovascular diseases. By analyzing vast datasets, including electronic health records and genetic information, AI models can predict individuals' risk of developing cardiovascular diseases. This predictive capability enables targeted preventive measures and personalized treatment plans, improving patient outcomes[30].

4.2. Limitations and biases

Despite these successes, the application of AI in cardiovascular medicine has been hampered by significant limitations, particularly biases that affect diagnostic accuracy across racial and ethnic groups[31]. Studies have demonstrated that AI models can exhibit biases that lead to discrepancies in

[27] It should be noted that the relationship between law and new technologies is typically defined by the legislator's delay: cf. R. Rolli, *Il Diritto privato nella società 4.0*, Milano, 2018, XVIII-XIX and M. Pietrangelo, *La società dell'informazione tra realtà e norma*, Milano, 2007, 176.

[28] M. Naghavi, K. L. Ong, A. Aali, H. S. Ababneh, Y. H. Abate, C. Abbafati, R. Abbasgholizadeh, M. Abbasian, M. Abbasi-Kangevari, H. Abbastabar, S. Abd ElHafeez, M. Abdelmasseh, S. Abd-Elsalam, A. Abdelwahab, M. Abdollahi, M. Abdollahifar, M. Abdoun, D. M. Abdulah, A. Abdullahi, C. J. L. Murray, *Global burden of 288 causes of death and life expectancy decomposition in 204 countries and territories and 811 subnational locations, 1990–2021: a systematic analysis for the Global Burden of Disease Study 2021*, in *The Lancet,* 403, 2024.

[29] Y. R. Wang, K. Yang, Y. Wen, P. Wang, Y. Hu, Y. Lai, Y. Wang, K. Zhao, S. Tang, A. Zhang, H. Zhan, M. Lu, X. Chen, S. Yang, Z. Dong, Y. Wang, H. Liu, L. Zhao, L. Huang, S. Zhao, *Screening and diagnosis of cardiovascular disease using artificial intelligence-enabled cardiac magnetic resonance imaging*, in *Nature Medicine*, 2024.

[30] D. Gala, H. Behl, M. Shah, A. N. Makaryus, *The Role of Artificial Intelligence in Improving Patient Outcomes and Future of Healthcare Delivery in Cardiology: A Narrative Review of the Literature*, in *Healthcare*, 12(4), 2024, 481.

diagnostic accuracy[32]. For example, an AI system developed for diagnosing heart disease showed higher sensitivity in identifying conditions in White patients compared to Black patients[33]. This discrepancy arises from the model being trained predominantly on data from White individuals, leading to less accurate predictions for other racial groups. The legal and ethical implications of such biases are profound. From a legal perspective, these biases may violate principles of non-discrimination and equity, as enshrined in regulations like the GDPR and forthcoming EU regulations on AI. Ethically, they raise concerns about fairness and the moral obligation to provide equitable healthcare services to all patients, irrespective of their racial or ethnic background.

4.3. Ethical and legal implications

The existence of bias in AI models used in cardiovascular medicine indicates the urgent need for frameworks that ensure the ethical development and deployment of AI. Legally, it necessitates adherence to principles of fairness and equity, requiring that AI models be developed and tested on diverse datasets that accurately reflect the population's heterogeneity. Ethically, it demands a commitment to minimizing harm and ensuring that AI technologies benefit all segments of society equally. To address these challenges, it is crucial to implement bias detection and mitigation strategies throughout the AI development lifecycle. This includes diversifying training datasets, employing fairness-enhancing algorithms, and conducting rigorous testing across diverse population groups. Additionally, transparency in AI development processes and outcomes is essential to build trust and ensure accountability.

5. Compliance and mitigation strategies

Ensuring compliance with the intricate web of legal requirements and ethical guidelines for the use of AI in healthcare is a complex yet crucial task. Central to this effort is adherence to the GDPR for entities operating within or dealing with data from the European Union, which mandates strict data protection and privacy practices. Similarly, international standards such as those developed by the International Organization for Standardization (ISO) offer guidance on maintaining data security, quality, and interoperability in AI systems. These frameworks, alongside various national and international guidelines, establish a foundation for ethical AI use that respects privacy, ensures fairness, and promotes transparency.

[31] Z. Javed, M. Haisum Maqsood, T. Yahya, Z. Amin, I. Acquah, J. Valero-Elizondo, J. Andrieni, P. Dubey, R. K. Jackson, M. A. Daffin, M. Cainzos-Achirica, A. A. Hyder, K. Nasir, *Race, Racism, and Cardiovascular Health: Applying a Social Determinants of Health Framework to Racial/Ethnic Disparities in Cardiovascular Disease*, in*Circulation: Cardiovascular Quality and Outcomes*, 15(1), 2022.

[32] E. Tat, D. L. Bhatt, M. G. Rabbat, *Addressing bias: artificial intelligence in cardiovascular medicine*, in *The Lancet Digital Health*, 2(12), 2020.

[33] D. Kaur, J. W. Hughes, A. J. Rogers, G. Kang, S. M. Narayan, E. A. Ashley, M. V. Perez, *Race, Sex, and Age Disparities in the Performance of ECG Deep Learning Models Predicting Heart Failure*, in *Circulation: Heart Failure*, 17(1), 2024.

For healthcare institutions and companies aiming to align their AI systems with these requirements, a multifaceted approach to compliance and bias mitigation is essential. This begins with the comprehensive mapping of AI applications against existing legal frameworks to identify specific compliance obligations. Following this, a thorough risk assessment process can highlight potential areas where AI systems might breach data protection norms or introduce bias in healthcare delivery.

Tools that can be used to enhancing protection of personal rights are the so-called privacy enhancing technologies ("PETs"). PETS are a collection of digital solutions aim at collecting, processing, analysis and sharing information while protecting the confidentiality of personal data[34][1]. PETs can be divided into three categories: data obfuscation, encrypted data processing, and federated and distributed analytics. Data obfuscation tools include zero-knowledge proofs (ZKP), differential privacy, synthetic data, anonymisation and pseudonymisation tools. These tools increase privacy protections by altering the data, by adding "noise" or by removing identifying details. Among them, differential privacy has been successfully applied to several large-scale biomedical data sharing initiatives, including the UK Biobank and the National Institutes of Health's All of Us research program. Concurrently, synthetic data has emerged in the healthcare sector as a powerful tool for analysis and technology development[35]. Synthetic data are data created from real datasets with similar statistical properties, enhancing privacy while allowing researchers to conduct meaningful analyses. This approach has been utilized in various contexts, such as simulation and prediction research[36], algorithm testing[37], public health research[38], and so on. Encrypted data processing tools include homomorphic encryption, multi-party computation, and trusted execution environments. Encrypted data processing PETs allow data to remain encrypted while in use (in-use encryption) and thus avoiding the need to decrypt the data before processing. For example, encrypted data processing tools were widely deployed in Covid tracing applications. Federated and distributed analytics, including federated and distributed learning, allows executing analytical tasks upon data that are not visible or accessible to those executing the tasks. In federated learning, for example, a technique gaining increased attention, data are preprocessed at the data source. In this way, only the summary statistics/results are transferred to those executing the tasks.

Another effective strategy for mitigating these risks is the incorporation of privacy by design principles from the outset of AI system development[39]. This approach ensures that data protection measures are not afterthoughts but are integrated into the core architecture of AI applications. Similarly,

[34] OECD, *Emerging privacy enhancing technologies current regulatory and policy approaches*, in *OECD digital economy papers*, 351, March 2023.

[35] A. Gonzales, G. Guruswamy, S. R. Smith, *Synthetic data in health care: A narrative review*, in *PLOS Digit Health*,2, 1, 2023.

[36] P. Davis, R. Lay-Yee, J. Pearson, *Using micro-simulation to create a synthesised data set and test policy options: The case of health service effects under demographic ageing,* in *Health Policy*, 97, 2–3, 2010, 267.

[37] C. Ngufor, H. Van Houten, B. S. Caffo, N. D. Shah, R. G, McCoy R.G., *Mixed effect machine learning: A framework for predicting longitudinal change in hemoglobin A1c*, in *Biomed Inform.*, 89, 2019, 56–67.

[38] W. T. Enanoria, F. Liu, J. Zipprich, K. Harriman, S. Ackley, S. Blumberg, *The Effect of Contact Investigations and Public Health Interventions in the Control and Prevention of Measles Transmission: A Simulation Study*, in *PloS One*, 11, 12, 2016.

[39] S. Reddy, S. Allan, S. Coghlan, P. Cooper, *A governance model for the application of AI in health care,* in *Journal of the American Medical Informatics Association*, 27, 3, 2020, 491–497.

implementing rigorous data governance policies helps safeguard patient information, ensuring that data collection, storage, and processing activities comply with legal standards.

Bias mitigation requires a proactive stance, starting with the diversification of datasets to reflect the heterogeneity of the population accurately. This involves not only the inclusion of diverse demographic groups in the data but also the careful annotation of data to identify potential sources of bias. Advanced analytical techniques can then be employed to detect and correct for biases, ensuring that AI models perform equitably across different patient groups.

Beyond technical measures includes regular training for staff on the ethical implications of AI and the establishment of clear guidelines for responsible AI research and development. Ethical review boards, similar to those used in medical research, can provide oversight for AI projects, evaluating them for potential ethical concerns and compliance with legal standards.

Public research bodies and corporate entities alike must integrate these legal and ethical considerations into their AI development processes through continuous engagement with stakeholders, including patients, healthcare professionals, and legal experts. Such engagement ensures that AI systems are developed with a clear understanding of the legal landscape and ethical expectations, facilitating compliance and promoting the responsible use of AI in healthcare.

Through these strategies, organizations can navigate the complexities of AI compliance, transforming legal and ethical challenges into opportunities for innovation in healthcare. By prioritizing data protection, bias mitigation, and ethical considerations, healthcare institutions and companies can leverage AI to enhance patient care, improve healthcare outcomes, and uphold the highest standards of fairness and respect for patient privacy.

6. Bridging the gap: from regulation to practice

The task of aligning the regulatory corpus with the practical exigencies of health research and service delivery is a complex yet essential undertaking for entities operating within the health sector. This alignment is necessary not only for ensuring legal compliance but also for harnessing the full potential of AI in advancing healthcare. To bridge this gap effectively, a comprehensive approach that encompasses policy development, stakeholder engagement, and the establishment of robust oversight mechanisms is required.

Entities can begin by conducting a thorough analysis of how existing regulations impact their operations and identifying any areas where AI applications could potentially lead to non-compliance or ethical dilemmas. This initial assessment should serve as the basis for developing tailored AI governance policies that address specific regulatory and ethical concerns while also meeting the operational needs of healthcare delivery. Such policies should outline clear procedures for data handling, consent management, algorithmic transparency, and bias mitigation, ensuring that all aspects of AI use are covered.

Engagement with stakeholders is another fundamental aspect of bridging the regulatory and practical scenario. This includes not only healthcare professionals and patients but also legal experts, ethicists, and regulators. By fostering open dialogues, entities can gain diverse perspectives on the practical challenges of implementing AI in healthcare settings, identifying common concerns and collabora-

tive solutions. Stakeholder input can also guide the development of AI applications that are not only compliant with legal and ethical standards but are also aligned with patient care priorities and clinical needs.

To sustain compliance and address ongoing legal, ethical, and practical challenges, a dynamic framework for the monitoring and assessment of AI systems in healthcare is indispensable. Such a framework should include:

- Continuous Monitoring: Regular audits of AI systems to ensure they operate as intended and do not deviate from compliance requirements or ethical norms. Monitoring should also include the tracking of data sources and algorithmic decisions to identify any emergent biases or privacy concerns.
- Impact Assessment: Periodic evaluations of the impact of AI applications on patient outcomes, healthcare equity, and operational efficiency. These assessments can help identify areas where AI is delivering value, as well as those where it may be falling short or inadvertently introducing disparities.
- Adaptive Governance: Mechanisms for revising AI policies and practices in response to new regulatory developments, technological advancements, or changes in healthcare delivery models. Adaptive governance ensures that AI applications remain relevant and beneficial in the face of evolving healthcare landscapes.
- Stakeholder Feedback Loops: Regular opportunities for feedback from healthcare professionals, patients, and other stakeholders to inform the ongoing development and refinement of AI applications. This feedback can provide practical insights into how AI is affecting healthcare delivery and patient care, guiding improvements and adjustments.

By implementing such a framework, entities in the health sector can navigate the complexities of applying AI in healthcare, ensuring that their innovations not only comply with legal and ethical standards but also meet the practical needs of health research and service delivery. This approach fosters an environment where AI can be leveraged responsibly and effectively to improve health outcomes, enhance patient care, and advance the frontiers of medical knowledge.

7. Conclusions

The integration of AI into healthcare holds the potential to transform not only patient care, but also medical research profoundly. However, realizing this potential fully requires us to navigate the complex landscape of legal and ethical challenges diligently.

Effective and non-formal compliance is necessary to maximize the potential of AI in healthcare data processing and capitalize on all opportunities for risk management, beyond simply complying with regulatory requirements.

Therefore, it is becoming increasingly necessary not only to operate from a privacy by design perspective, but to integrate this one with the AI regulatory framework, although not yet applicable.

Taking a proactive approach towards the AI Act, considering it already as a reference model despite not being entirely binding yet, represents a forward-looking and future-proof strategy for the integration of AI technologies

Furthermore, by pushing collaboration among all stakeholders involved and committing to ongoing research and dialogue, we can ensure that AI serves as a force for good in healthcare, enhancing the wellbeing of individuals and communities worldwide. This balanced approach to innovation will pave the way for a future where AI not only revolutionizes healthcare but does so in a manner that is just, equitable, and respectful of the rights and dignity of all individuals.

Addressing the legal and ethical implications of AI in healthcare, specifically in health research, is vital for ensuring that these technologies benefit all patients equally. By implementing robust compliance and bias mitigation strategies, healthcare institutions and companies can leverage AI and research findings achieved through such systems to enhance patient care, improve health outcomes, and uphold the highest standards of fairness and privacy. The ongoing collaboration between stakeholders, including regulators, healthcare professionals, and patients, will be crucial in the complexities of AI integration and fostering an environment where AI can be used responsibly and effectively to advance medical knowledge and healthcare delivery.

ISSN 2284-4503