Analysing The Dynamic Nature Of AI In Healthcare And The Legal Landscape

---

Table of Contents

Abstract

It is an in-depth study of the applications of Artificial Intelligence (AI) technologies such as Machine Learning (ML) and Natural Language Processing (NLP) in healthcare sector to expand diagnostic capabilities. It also examines the use cases of AI in healthcare, delving into the legal ramifications with an emphasis on critical issues such as patient data privacy and relevant privacy laws in real world settings. The challenges of safeguarding data privacy, alongside issues in medical liability, ethical considerations, including informed consent, fairness, and algorithmic biases are analysed to underscore the responsible use of patient data. Additionally, this paper addresses cross-jurisdictional legal complexities affecting Artificial Intelligence in healthcare by assessing global regulatory perspectives, specifically the initiatives by the United States, the European Union, and India's current developments and frameworks that promote secure and ethical integration of AI technologies in healthcare. This study concludes with recommendations for the safe deployment of AI in this domain.

Keywords–Machine Learning, Natural language processing, Artificial Intelligence, European Union, United States, India, Cross-jurisdiction.

1. Introduction

Artificial Intelegence has become equivalent to human intelligence. A revolution in healthcare has started with new AI-driven applications. AI is changing the way professionals diagnose, treat, track patient progress, disease detection and manage patient care. It has potential to influence clinical decision-making, improve operational efficiency and provide personalised treatment plans. The growing use of AI is also leading to many serious challenges and concerns, such as ethical, legal and regulatory concerns including the safe and effective use of AI technologies. **Data breaches has also become one of the serious concerns in India. According to the reports around 2,138 cyber-attacks per week[1] and 15% increase from the previous year, positioning India as the second most targeted nation in the Asia Pacific region.** U.S. has FDA, a federal agency to regulate AI driven medical devices through process of multiple testing, EU has GDPR to regulate the use of personal data whereas **India's uniform regulatory framework is at a developmental stage and focusing more towards Data privacy.** The Information Technology Act 2000, and the Sensitive Personal Data or Information Rules are currently applied to regulate data privacy in healthcare; however, they fall short of addressing the specific challenges related to patient data regulation and privacy.

[1] "Indian organizations hit by 15% more weekly hackings in 2023", Times of India – Jan 2024.

Background of AI in Healthcare

It was in the late 1970s that AI was first used in medicine to deal with biomedical problems and later led to interpreting electrocardiograms (ECGs) which record the electrical activities of the heart and helps in decision-making. During this period the biomedical applications of AI emerged and catalyzed in part by the creation of a computing network designed for developing AI applications in the biomedical sciences called SUM EX-AIM. Since then, AI has transformed with the integration of machine learning and deep learning and functions on huge datasets, including clinical data and electronic health records. AI assists in diagnosing patterns and predicting outcomes, facilitating earlier diagnosis, prior health alerts and more personalized treatment strategies. **The AI market in the health sector is predicted to grow at a compound annual growth rate of 47.6% from 2023 to 2028 and reach a value of $102.7 billion in 2028[2].**

AI has become more powerful and dominant in this morden era. In various healthcare functions, including diagnostics, medical imaging, and drug discovery AI is playing its vital role. As evidenced by Absci corporation, a generative AI drug creation company, was the first entity to create and validate de novo antibodies using AI and patient monitoring[3]. Since then, it has continued to evolve as AI technologies are being implemented in everyday medical practices. The impact of AI will expand in the coming ages, with improved accessibility of medical services.

Purpose and Scope of the Research

This study aims to provide an in-depth analysis of emerging AI technologies in healthcare from its past to present including the overview of AI technologies used currently in healthcare, the legal and ethical considerations, including data privacy, liability, and regulatory frameworks; and global perspectives on AI in healthcare regulations. This research paper is to identify AIs' positive and negative sides, exploring the effects of AI on patient autonomy, informed consent, and potential biases in algorithmic decision-making. Furthermore, it will analyze one of the many complicated or unexpected results of a decision on AI integration in a legal framework, including patient data privacy and the evolving landscape of intellectual property rights related to AI innovations.

---

[2] Vindal, Vipin. 2024. "Future trends and opportunities at the intersection of AI & healthcare/pharma." Express Computer.

[3] Absci First to Create and Validate De Novo Antibodies with Zero-Shot Generative AI | Absci Corp." 2023. Investor Relations | Absci Corp.

2. Overview of AI Technologies in Healthcare

Artificial Intelligence(AI) can perform tasks that typically require human intelligence. These tasks include learning, reasoning, problem-solving, providing solutions, understanding natural language, converting complex data into simple ways and adapting to new information for accurate data processing. Artificial Intelligence(AI) copies human intelligence and functions on neural networks. The core of deep learning centers around the neural networks with multiple layers of human brain cognitions. These networks can automatically identify confusing patterns from extensive datasets, enabling advanced capabilities like image recognition and natural language processing, and can apply in a modular design to improve products and systems.

I. Types of AI in healthcare sector

Technologies

AI technologies are used in many healthcare branches like clinical, pharma, and administrative to diagnose diseases. Several AI applications like **Google's DeepMind AI can detect disease in less time with great accuracy. DeepMind can predict acute kidney injury (AKI) 48 hours before it occurs with 90% accuracy[4].** IBM's Watson takes a range of genetic information and can analyze patient records and suggest personalized treatment plans[5].

AI technologies used in the healthcare sector.

1. Machine Learning

   Machine learning (ML) is also called a "**Smart Machine**". Deep learning is one of the subsets of ML. It can learn from data without any programme interface or input. The neural network, built through the deep learning process, helps it to analyze data of patients' past treatments and results and provides decisions and predictions; the more data the ML algorithm gets, the more effectively, and accurately it delivers the results.

[4] Suleyman, Mustafa, and Dominic King. 2019. "Using AI to give doctors a 48-hour head start on life-threatening illness." Google DeepMind.

[5] "Announcements." 2018. IBM India Newsroom - Announcements.

ML is being widely used in following domain

a. Diseases Identification and diagnosis.
b. Drug Discovery and Manufacturing.
c. Medical Imaging.
d. Personalized Medicine and Treatment.
e. Disease Prediction.
f. Smart Health Records.

For instance, AI has been trained to detect deviations in cells such as cancer and malicious tumors, **AI can detect cancers and tumors at their early stage[6].**

2. Natural Language Processing (NPL)

It enables computers to interpret human language and manages unstructured data. It is the combination of advanced algorithms and machine learning. In healthcare, it works in two main tasks:

a. Speech recognition.
b. Unstructured Data Processing.

NLP algorithms take information from Electronic Health Records (EHRs) or medical documents, then process this information through techniques such as Optical Character Recognition (OCR), Named Entity Recognition(NER) and topic modeling and arrange data into groups and subgroups.

II. AI use cases in healthcare

The development of Artificial intelligence in India is at a very early stage, particularly in the form of clinical interventions. There are many identified use cases at the development and testing stage. Many use cases involve decision support systems, virtual assistants and process optimization. Computer vision is one of the advanced applications of AI that is being used to train AI algorithms to read X-rays and scans to support the processes of disease detection and diagnosis. There are only a few companies which are developing surgical stimulators, personalized health solutions and patient monitoring systems. A few interventions use Natural Language Processing and speech recognition, which are critical for meeting diverse linguistic and literacy needs in the country. This is going to change the **growing investments by big tech actors.**

[6] "NHS AI test spots tiny cancers missed by doctors." 2024. BBC.

Google[7], Microsoft[8] and IBM[9] have multiple partnerships with private hospital groups such as Narayana, Apollo and Fortis, along partnerships with state governments in India.

Some areas in which interventions are being developed are as follows:

a. **Disease Detection and Diagnostics**

Decision support systems for diagnostics and predictive systems for prognostication (an indication in advance) are being developed using Machine Learning. Deep Learning and computer vision models are used to read medical scans such as X-rays, CT scans, PET scans and Ultrasound scans. **AI-based systems are being used for early detection of tumors such as non-invasive, non-touch and non-radiation approaches to detect breast cancer as well as predicting cancer recurrence through a risk score[10].** AI-driven applications are also being developed and used for building systems that can analyze images of blood. Sig Tuple, a medtech startup, for example, is using an AI platform called Manthana for automated analysis of blood smears as well as for the digitization of blood, urine and semen samples. **In one of India's leading government hospitals, researchers have developed a tool that leverages thermal imaging and AI-based tests to help predict the onset of haemodynamic shock[11].** AI systems for tuberculosis diagnosis and DR systems are also being developed. OnliDoc and Lybrate platforms have started using AI methods to provide virtual assistance and diagnostics through online mode[12]. AI for symptom checking and treatment selection is used by OnliDoc[13].

b. **Process Optimization**

For the development of new efficiencies in the areas such as hospital bed management and the processing of insurance claims, Machine Learning(ML) is

[7] "Apollo Hospitals expands partnership with Google Cloud to boost the healthcare ecosystem in India. - Apollo Hospitals." 2023. Apollo Hospitals.

[8] "Microsoft & Apollo Hospitals to use Artificial Intelligence for early detection of cardiac diseases - Microsoft Stories India." 2018. Microsoft News.

[9] "Announcements." 2018. IBM India News Room - Announcements.

[10] Conner, Kristine. 2024. "Using AI (Artificial Intelligence) to Detect Breast Cancer." Breastcancer.org.

[11] Rhythma Kaul. 2019. "AI-based tests to help detect shock in children could save many lives." Hindustan Times.

[12] Divedi, Vinay. 2016. "Startup Lybrate's online doctor consultation platform expands healthcare access. The Economic Times.

[13] Misal, Disha. 2018. "11 Indian Startups Revolutionizing The Healthcare Sector With AI." Analytics India Magazine.

being used. A few online platforms that assist to help find a doctor, storing health records, or procuring medicine are using ML to improve efficiencies in these processes. Others are automating the first-level screening of symptoms, finding doctors and booking appointments. Optical character reading systems are also used to scan prescriptions and check prescribed medications against the inventory. ML is also being developed for food bed management and planning, to predict rates of patient churn (turnover of beds), and to optimize the use of beds in hospitals.

c. Patient facing applications

Chatbots are increasingly being used as conversational agents for interaction with patients. More than 15,00 cases per month, for example, is handled by the online platform named mfine, approximately the number of patients handled by Manipal Hospitals, one of Bangalore's largest conventional hospital groups[14]. To schedule appointments, converse, and collect basic details and symptoms, several large hospitals now use chatbots. **To address loneliness and mental health, chatbots are being used as the first level of intervention in behavioral coaching. Patient recovery monitor applications are also under development**. AI-driven analysis of camera feeds is being used to detect emotional responses and patient fatigue, to help monitor patients during the treatment process and to alert medical staff. Sensor data monitors patient recovery and response to medication after surgery or treatment. Development of Wearable sensors and AI-based solutions are being done to measure vital signs and provide doctors with actionable insights. While at a much earlier stage of development, Deep Learning techniques are being developed to derive molecular insights for drug discovery. **Surgery simulators[15] are continually updated and developed to train doctors for spine and knee surgery. A surgery simulator center was recently opened in Delhi[16].** Within research institutions, non-profit organizations, and medical service providers, primary data are the main source. Through other platforms or healthcare services, data are collected by developers, for example, a healthcare platform which enables doctor discovery, online consultations and online medical purchases would employ user data captured on

[14] Arihant Patni. 2021. "How AI Will Continue To Alter The Healthcare Landscape In 2021 & Beyond." Linkedin.

[15] PTI. 2016. "Open Ortho Surgery Simulator based on AI launched in India." Times of India.

[16] "AIIMS to launch surgical robotics training facility for resident doctors, faculty today." 2023. The Indian Express.

their platform to build an AI system to optimize and automate certain operations pipelines doctor The main sources of data for developing these systems are primarily historical data held within research institutions, non-profit organizations and medical service providers.Through other platforms or healthcare services in some cases developers collect data, for patient matching, and doctor discovery based on location data in their services.

Open-source data are generally used by the developers to get the model off the ground in cases where the models need to be trained on more general aspects, such as conversational ability or image recognition. **Start-ups often use publicly available datasets from the US and Europe, as India does not have robust medical datasets.[17] Developers also use models available with cloud providers such as Google, Microsoft and Amazon incase of AI algorithm is a small part of their systems, or they do not possess in-house capabilities.** Startups like Wadhwani AI are creating on field data sets to decrease dependency on the datasets from other countries. Wadhwani AI is developing an AI model to estimate child weight by assessing pictures of infants, aiding public health and reducing neonatal risks[18].

A few start-ups and initiatives have begun to provide personalized health solutions. A digital health and wellness start-up in Bangalore, called Healthi, uses predictive analytics, personalization algorithms and Machine Learning to deliver personalized health suggestions.[19] Similarly, **Manipal Hospitals is using IBM Watson for Oncology, a cognitive-computing platform, to help physicians discover personalized cancer care options.[20]**

3. Navigating Challenges and Frameworks in India

I. Patient Data Privacy

Data privacy has increasingly become a matter of concern in the area of AI-driven healthcare, in which a large amount of data is used to generate results and outcomes.

[17] Pradhan, Keerti. n.d. "Use of artificial intelligence in healthcare delivery in India." Journal of Hospital Management and Health Policy.

[18] Tapaswi, Makarand. n.d. "Maternal, Newborn, and Child Health: AI Solutions." Wadhwani AI. Accessed October 21, 2024.

[19] Salvi Mittal. 2017. "healthi.in leverages predictive analytics & machine learning for preventive. ET.CIO

[20] "Manipal Hospitals tap IBM Watson." 2015. Healthcare IT News

Patients provide their data in response to the benefits of their health, not to be sold or used against them. **AI systems require a set of primary data to learn the algorithm, such as medical data, diagnosis, treatment plans and clinical data including Personally Identifiable Information (PII) and Protected Health Information (PHI), which should be protected under the law**. In India, cyberattacks in healthcare have increased rapidly in the last couple of years. An **attack by the ALPHV Ransomware Group on Sun Pharmaceuticals, AIIMS cyber-attack, and Safdarjung Hospital's hacking attack.** On 6 June 2023, **AIIMS Delhi witnessed a malware attack, which was detected at 1450 hours by the cybersecurity systems deployed in the institute.**[21]Hackers use sensitive information to impersonate victims, open bank accounts and also taking loans on their names. Stolen data can be used to craft convincing scams, victims may spend years in recovering from financial fraud or identity theft.

The adoption of technology has changed the healthcare system, now-a-days patients no longer have to collect and preserve physical reports. Life has become much easier with telemedicine, IoT devices, electronic health records (EHR),but it has given rise to a new menace: theft of sensitive patient data. **India's healthcare industry has become a prime target for cybercrimes, facing approximately 6,900 attacks each week**[22]. This leads to the requirement of a stronger cybersecurity infrastructure and with this alarming trend demonstrates the evolving complexities in ensuring data privacy and security in the healthcare sector. As developments of AI in healthcare will lead to an increase in data breaches.

II. Overview of Privacy Laws

In AI driven healthcare protection of privacy and patient rights are the most challenging aspects, such as the right to informed consent and the right to medical data protection, and these concerning areas have brought the need for laws and regulations. **AI studies should be transparently reported to have value to inform regulatory approvals**. **India's present legislative framework has only two provisions such as the IT Act and the SPDI Rules. It focuses on the protection of collecting, disclosure and transfer of sensitive personal data such as medical records and**

[21] "AIIMS thwarts malware attack, no data breach." 2023. Times of India.

[22] Shah, Jainam. 2024. "India's healthcare sector top target of cybercrimes: Report." India Today.

histories and comprises India's general framework for data protection. It makes online transactions and electronic data transfers safe. The IT Act governs various internet activities, including the legal status of electronic records and the authentication of digital signatures, and covers a wide range of cybercrimes, including hacking and denial-of-service attacks. Furthermore, India enacted the DPDP Act, its key purpose is to increase accountability and responsibility for enterprises that operate in India, such as mobile app developers, internet service providers and companies that collect, store and handle personal data of Indian citizens. This Act, with a particular emphasis on the "**Right to Privacy**", strives to ensure that these companies function clearly and are accountable when it comes to handling personal data, therefore prioritizing Indian individuals' privacy and data protection rights. The Digital Information Security Act (DISHA), an ACT to provide National and State eHealth Authorities and Health information exchanges. It is to regulate the processes related to collection, storing, transmission and useof digital health data.**The government and the Ministry of Health and Family Welfare announced the National Digital Health Mission (NDHM) and published a blueprint recommending the establishment of a National Digital Health Ecosystem, enabling interoperability between digital health systems, hospital and ancillary healthcare-provider levels.[23] The large language models can overwhelm people with both accurate health information and also misinformation, leading to potential challenges in public health, and this becomes the need for policy and user guidance for AI-driven healthcare systems.**

III. Challenges in Data Privacy Management

There is a vibrant and complex array of challenges to gain patient trust, regulatory compliance, and effective healthcare delivery. The increased developments in AI-driven healthcare have made it crucial to navigate these challenges. It includes not only the records but also a large set of data including genetic information and personal identifiers, it becomes pivotal to maintain confidentiality, if not maintained properly then it will be vulnerable to misuse. The potential for breaches or unauthorized access raises serious privacy concerns. **The regulatory landscape that varies by jurisdiction should be followed by the healthcare organizations. Obtaining informed consent from the patient is a challenging aspect of data privacy management. The patient needs to understand how their data is being utilized,**

[23] 2019. Government and the Ministry of Health and Family Welfare e-health section. Blueprint

especially in the context of AI algorithms which often operate as a black box. The implication of AI driven technologies in healthcare has become complex, especially when data is used for secondary research. The exchange of data poses another serious challenge in the realm of AI driven healthcare. The AI systems in various healthcare platforms often involves cluster of data from multiple sources, including electronic health records (EHRs), wearable devices, and imaging systems and variations in data formats, standards, and governance can complicate secure data sharing. **The data AI gets should represent accurate patient demographics because it makes decisions on the biases of the data provided.** In a hospital setting, patients usually don't know how predictive algorithms are created. It can unfairly code their algorithms to discriminate against minorities and prioritize profits rather than providing optimal care. So **it becomes crucial to ensure that the AI models are developed using privacy measures and not perpetuate bias.** The question of data ownership and control further complicates privacy management. Lastly, **resource constraints can hinder effective data privacy management. Many healthcare organizations, especially smaller ones, may lack the necessary resources and expertise to implement robust data privacy strategies. This inadequacy can lead to insufficient protections and an increased risk of non-compliance with data protection regulations.**

IV. Medical Liability in Healthcare Management by AI

Medical Liability is a legal responsibility of healthcare providers to harm caused to a patient due to their actions or in the failure of diagnoses. This concept is rooted in the principle that healthcare professionals owe a duty of care to their patients and mandatory delivery of treatment and medical services by established standards of practice in the medical community. In healthcare settings AI poses a host of legal and ethical questions, especially regarding the attribution of medical liability, and it exists whenever damage occurs without proving fault on the part of the defendant.

Fault-based liability, dilutes responsibility, creating a lenient path for AI platforms and tools to avoid accountability and it also has implications for healthcare providers, manufacturers, and patients. The another type of liability is strict liability which has accountability for harm caused by hazardous products, regardless of fault and could ensure higher standards for AI-driven medical devices but complicates their deployment. While strict liability is fitting for dangerous products, it may seem extreme

for medical devices, which is aimed at improving treatment quality. The legal framework of negligence and fault-based liability (medical malpractice), seems increasingly applicable as AI technologies are becoming advanced with autonomous functions and complex outputs. This fault-based approach may better put up Artificial Inteligence in healthcare, even if it risk reducing the accountability of powerful, autonomous technologies that could potentially cause unforeseen harm.

Table 1. Examples of outcomes related to AI use in clinical practice for doctors

No	**AI recommendation**	**AI accuracy**	**Doctor action**	**Patient outcome**	**Legal outcome (probable) for the doctor**
1.	Standard of care	Correct	Rejects	Bad	Injury and Liability
2.		Incorrect	Follows	Bad	Injury but no Liability
3.	Non-standard care	Correct	Rejects	Bad	Injury but no liability
4.		Incorrect	Follows	Bad	Injury and Liability

These results suggest that, **regardless of the accuracy or inaccuracy of the AI diagnosis, doctors are held liable only when they deviate from the standard of care. The current view reinforces that doctors are primarily accountable for adhering to established standards, providing a degree of consistency and predictability in legal outcomes.** On the other hand, some may argue that the liability system should consider the accuracy of AI diagnoses as a factor in determining physician omissions. It could be relevant particularly in situations where AI outperforms the standard of care. This raise questions about the adaptability of legal frameworks to advance the technologies. The issue of product liability adds another layer of complexity, which applies to the manufacturers of finished products consisting of software and hardware. The applicability in cases involving AI-undermined algorithms which themselves can be considered products under the existing liability laws complicates the need to understand how responsibilities divide when AI systems are used in healthcare operations. Vicarious liability is another kind of liability, in which providers are accountable for the actions of AI-driven devices deployed in their facilities. The costs associated with patient injuries caused by these technologies are shared among all parties involved, providing complete compensation to those affected.

Table 2. Overview of liability

Type of liability	**Person liable for the damage**	
	Healthcare Institution	**Producer of AI**
Vicarious liability of a healthcare institution (medical malpractice)	Doctor's failure to follow the duty of care	Not applied
Corporate negligence of healthcare institution	Poor organisation of the service of the healthcare institution	Not applied
Producer's liability for defective products	Not applied	Producer's failure to provide a proper product

As AI is transforming the healthcare sector, it is not yet clear that AI systems should be considered as agents or employees, this further complicates the process of establishing clear lines of responsibility and accountability when it comes to any injury caused by AI technologies.

Indian case law addressing AI applications in healthcare remains limited, as the regulatory framework is still developing. However, certain cases and discussions highlight the issues related to AI-driven medical devices, safety, and accountability.

VI. Intellectual Property Rights and AI Innovations.

Artificial intelligence (AI) is pushing innovation in new ways and accelerating with technological advancements in computing power, data and algorithms, leading to the ability to use AI tools in previously unachievable ways. This has increased AI deployments by companies ranging from startups to long-established institutions. **Intellectual property (IP) protects and encourages innovation and creativity and in the current industrial and market scenario, clear ownership of Intellectual Property ("IP") is paramount and ownership of such IP is of utmost importance.** While discussing ownership, the biggest point of debate is whether ownership can be extended to a non-human counterpart such as software, algorithms, etc. which contributed to the development of a product. **The current IP law in India does not have express provisions for extending recognition, much less ownership, to software and algorithms that are used to create IP eligible for statutory protection and the exception to this is a limited extent, can be found**

under the Copyright Act of 1957[24], which recognises a person who causes the computer-generated work to be created as the author [**Section 2(d)(vi) of Indian Copyright Act, 1957**]. **The Patent Act, of 1970** and **the Design Act, of 2000**[25] do not have any provisions to recognise a programmer as the owner of any innovation that results from the operation of any software algorithms, with comparison to Indian legislation with foreign legislation, it is noted that even the UK expressly provides[26] for copyright protection of computer-generated works that do not have a human creator and **the Copyright under section 9 (3) Designs and Patents Act (CDPA)** mentions that In the case of a literary, dramatic, musical or artistic work which is computer-generated, it shall be taken to the person by whom the arrangements necessary for the creation of the work are undertaken, and under **section 178 of the CDPA** defines a computer-generated work as one that is generated by computer in circumstances in which there is no human author of the work. CDPA and similar legislative provisions were also inspired and adopted by New Zealand and Ireland's legislations, **Presently, the legal framework in India has held with the Patents Act of 1970 and the Copyright Act of 1957, does not adequately address the intricacies of inventorship, authorship, and ownership concerning works created independently by Artificial Intelligence.**

4. Ethical Considerations in AI Driven-Healthcare.

I. Informed Consent and Patient Autonomy.

Patient autonomy and obtaining informed consent in AI-driven healthcare face many challenges. Obtaining informed consent for AI systems demands clear and concise communication about how the AI will be used and what its potential impact may be and understanding how their data will be used by AI applications, becomes challenging for patients, this also raises concerns surrounding the data privacy and the increased issue of the expiration of informed consent and tackling problems.

II. Algorithmic Bias and Fairness.

AI bias is referred to as "**the application of an algorithm that compounds existing inequities in socioeconomic status, race, ethnic background, religion, gender, disability, or sexual orientation and amplifies inequities in health systems.**" AI

[24] "(14 OF 1957)." n.d. Copyright Office. Accessed October 22, 2024.

[25] "The Designs Act 2000 | Intellectual Property India." 2019. Indian Patent Office.

[26] Erickson, Kristofer. 2024. "Copyright protection in AI-generated works." Creative Industries Policy and Evidence Centre.

bias is **often associated with data generalizability** when the data used to train an algorithm is not representative and thus the outputs cannot be generalized confidently or safely. There are many other ways, bias can be introduced and encoded in the algorithms that drive AI technologies.

Below are several instances of algorithmic biases shown to have direct harmful impacts on the health and safety of patients:

a. In African American patient context, a widely used cardiovascular risk scoring algorithm was shown to be much less accurate because approximately[27] 80% of training data represented Caucasians.
b. **AI models that predict cardiovascular disease and cardiac events are less accurate in predicting these conditions among female patients if trained specifically on male data sets**[28].
c. In radionics[29]chest X-ray-reading algorithms trained primarily on male patient data were significantly less accurate when applied to female patients.
d. **Algorithms for detecting skin cancer are trained largely on data from light-skinned individuals, and are much less accurate in detecting skin cancer in patients with darker skin**.

There are many sources of AI biases such as **human biases built into AI design, the data generality problem and biased humans with incomplete data leads to algorithmic bias.**

III. Cross- Jurisdictional Legal Issues

AI models are trained with a huge dataset, if unprecedented data is added then it can perpetuate and worsen existing health disparities due to societal discrimination or small sample sizes. Patient data privacy, protection against harm and ensuring that patients have control over their data usage, all these are the challenges in AI-driven healthcare. Despite the promise of deep learning models in medical imaging and risk prediction, their lack of interpretability and explainability are major concerns, where transparency is crucial for clinical decision-making, so evaluation of guidelines for AI systems should

[27] "Overcoming AI Bias: Understanding, Identifying and Mitigating Algorithmic Bias in Healthcare." n.d. Accuray.

[28] "Artificial Intelligence and Cardiovascular Risk Prediction: All That Glitters is not Gold." n.d. National Library of Medicine.

[29] Wiggers, Kyle. 2020. "Researchers find evidence of racial, gender, and socioeconomic bias in chest X-ray classifiers." VentureBeat.

include assessing and collecting evidence on data quality to prevent unintended consequences and harmful outcomes. The following sections will elaborate on these principles and analyze how different countries are positioned concerning them.

a. **Documentation and Transparency**

   Transparency can be achieved through different levels including simulatability (human understanding of the model), decomposability (explaining model behavior and components), and algorithmic transparency (understanding the model's process and output). The EU AI Act is one of the strongest acts declaring the requirement of technical documentation for high-risk AI systems to enable auditing, monitoring and ensuring reproducibility of AI outputs and processes. Regulations in other countries speak to the same principle. In AI governance most of the laws mention transparency and explainability as their requirement. However, the definition of transparency varies from 'communication of appropriate information about an AI system to relevant people' in the UK to 'transparency of governance measures and systems used' in Brazil transparency is defined in a more structured manner in the context of the healthcare sector by Canada, defining transparency as "the degree to which appropriate and clear information of a device (that could impact risks and patient outcomes) is communicated to stakeholders".

b. **Risk Management**

   The National Institute of Standards and Technology (NIST) uses risk management as **coordinated activities** to direct and control an organization about risk. The International Telecommunication Union (ITU) Focus Group on Artificial Intelligence for Health elaborates on this thought by its recommendation of a risk management approach that addresses risks associated with cybersecurity threats and vulnerabilities, underfitting, algorithmic bias etc. Risks linked to cybersecurity and privacy are highlighted by the UK, while pre and post market surveillance is highlighted in Canada's approach towards medical devices. Rwanda Ministry of ICT and Innovation, Rwanda in 2020 and Egypt for Economic Co-operation and (OECD) in 2023 acknowledge AI risk assessment as a tool for responsible AI, while Singapore (HSA) in 2022 and **India of Medical Research (ICMR) in 2023, have published technical guidance on process controls and change management.** Saudi Arabia Food and (SFDA) in 2023, emphasizes involvement of a cross-functional team for performing risk management.

Data ecosystems and sharing of good-quality data sources of the healthcare system and national interoperability standards are exemplified by Austria. Japan and Rwanda also propose similar concepts. Japan has an important view of converting data in a form suitable for AI and the creation of data economic zones which is to enable the use of AI for healthcare applications. Rwanda proposes an implementation plan for the availability and accessibility of quality data through indicators such as the size of open AI-ready data. Data quality is essential for building accurate AI models, data management approaches are influenced by quality culture as an organization. The UK has a similar approach as it uses a data quality culture, action plans and root cause analysis to address data quality issues at the source. The Framework also speaks of data maturity models and metadata guidance to bring data quality to life. The European Health Data Space (EHDS-TEHDAS) data quality framework recommends more granular mechanisms of data quality management. Singapore [(HSA), Hong Kong and **India [of Medical Research (ICMR)] also discuss the quality of learning and training datasets for accurate validation.**

c. **Privacy and Data Protection**

There have been several laws passed in the spirit of privacy and data protection, with the EU GDPR coming into effect in 2018 and its data protection by design is being echoed by other nations as well, such as **India's proposed data privacy by design policy.** A popular approach, privacy impact assessments, for proactive privacy risk assessment and mitigation, are frequently included in privacy frameworks. The European Health Data Space (EHDS) seeks to foster ownership of healthcare data by individuals and builds further on the GDPR. The health data as sensitive personal data or personally identifiable information that requires a high standard of safety and security is classified by the WHO Global Strategy on Digital Health(2020-2025). **India's ICMR guidelines call out no identity of data in line with the WHO strategy. However, the no-identity data does not guarantee privacy, with a study[30] showing how people can be re-identified from a no-identity data collection by providing their zip code, gender, and birthdate.** Singapore (HSA), emphasizes cybersecurity requirements for connected medical devices which focuses on design controls, test reports, and traceability. Additionally,

[30] Lubarsky, Boris. n.d. "Georgetown Law Technology Review." Georgetown Law Technology Review.

cybersecurity and privacy go hand in hand, an example being the UK's 'Plan for Digital Regulation'[31] and Saudi Arabia's Guidance on AI/ML based Medical Devices[32] focusing on infrastructure security.

5. Global Perspectives on AI in Healthcare Regulation

I. United States: FDA Regulations and Initiatives

The United States Food and Drug Administration (FDA or US FDA) is a federal agency of the Department of Health and Human Services, and it is responsible for protecting food security and medical devices. It was established under the Federal Food, Drug and Cosmetic Act of 1938 and its **primary focus is to protect public health by ensuring the safety and efficacy of the products. To regulate firms that manufacture, repackage, relabel, and import medical devices sold in the United States, the FDAs Centre for Devices and Radiological Health (CDRH) is responsible.** In addition, **CDRH regulates radiation-emitting electronic products (medical and non-medical) such as lasers, x-ray systems, ultrasound equipment, microwave ovens and color televisions**. Class I, II, and III are the classifications of the Medical Devices. The regulatory control increases from Class I to Class III, defining the regulatory requirements for a general device type. Class I devices are exempted from the premarket notification of 510(k). The premarket notification is in which any pharmaceutical product to enter the market, undergoes rigorous clinical trials meticulously evaluated by the FDA. The approval process is done with the focus of the 21st Century Cures Act and the FDA Modernization Act. Class II devices require Premarket Notification 510(k), and most of the Class III devices require Premarket Approval.

In U.S. the basic regulatory requirements that manufacturers of medical devices are listed below.

a. Establishment registration,
b. Medical Device Listing,
c. Premarket Approval or Premarket Notification 510(k), unless exempt.
d. Investigational Device Exemption (IDE) for clinical studies
e. Quality System (QS) regulation,

[31] "UK government publishes 'Plan for Digital Regulation.'" 2021. IAPP.
[32] Solaiman, Barry. 2024. "Regulating AI-Based Medical Devices in Saudi Arabia: New Legal Paradigms in an Evolving Global Legal Order." PubMed.

f. Labeling requirements, and
g. Medical Device Reporting (MDR)

Recently, on January 31, 2024, **FDA issued the Quality Management System Regulation (QMSR) Final Rule amends the device's current good manufacturing practice (CGMP) requirements of the Quality System(QS) regulation (21 CFR Part 820) which incorporates with the international standard specific for medical device quality management systems set by the International Organization for Standardization(ISO)**. This action is intended to harmonize the FDA's CGMP regulatory framework used by other regulatory authorities, this will be effective from February 2, 2026, onwards, two years after the publication till then, manufacturers are required to comply with the QS regulation.

II. European Union: GDPR and Regulatory Frameworks of AI

GDPR is an EU law with **mandatory rules for how organizations and companies must use personal data with integrity-friendly way.** Personal data means any information which, directly or indirectly, could identify a living person. Name, phone number, and address are schoolbook examples of personal data. Interests, information about past purchases, health, and online behavior are considered personal data as they could identify a person. Processing data, collecting, structuring, organizing, using, storing, sharing, disclosing, erasing and framing data. Each organization that processes personal data (every organization with employees and customers) must ensure that the personal data it uses fulfills the requirements of the GDPR.

The Practical Implications

a. Inform citizens and customers of your activities transparently
b. Assign a Data Protection Officer (DPO) to your organization, who should work as the main operator and the expert on your organizations' privacy work.
c. Manage the citizens' and individuals' rights efficiently. If a data subject contacts you to exercise their rights under the GDPR,
d. Regulate the responsibility between Buyer (Controller) and Supplier (Processor).
e. Data inventory. Each Controller and each Processor must keep a record of information on the use of data. The rules for the record of processing are specified in article 30 GDPR[33].
f. Set up processes to manage personal data breach within a 72-hour time frame.

[33] "Art. 30 GDPR – Records of processing activities - General Data Protection Regulation." n.d. GDPR.

g. Analyze possible risks and impacts on citizens' rights for the intended use of personal data. Data Protection Impact Assessment ("DPIA") and is set out in Article 35 GDPR.

A number of proposals on AI legislation have been discussed in the European Union, including several are described below.

1. Legislation on transparency of decision-making systems.
   Transparency is the key to ensuring that AI is not biased, and AI systems are explainable. For instance, the Finnish national AI strategy paper[34] recommends assessing how ethical obligations could be imposed on platforms, as is done in the GDPR. The paper focuses more towards certain parts of an algorithm developed and used by the platforms that could be prohibited if it distorts or restricts competition without justification. In July 2019, the EU adopted the new Regulation (EU) 2019/1150 requiring providers of online intermediation services and online search engines to implement a set of measures to ensure transparency and fairness in the contractual relations they have with online businesses (e.g. online retailers, hotels and restaurants businesses, app stores) that use such online platforms to sell and provide their services to customers in the EU. The Commission is also carrying out an in-depth analysis on algorithmic transparency. Against this background, a 2019 Parliament study recommends the creation of a regulatory body for algorithmic decision-making tasked with defining
   a. Criteria that can be used to differentiate acceptable algorithmic decision-making systems (that should be subject to an algorithmic impact assessment) and systems that should be prohibited.
   b. The obligations falling on algorithmic decision-making system providers (such as the obligation to make their systems auditable). New EU legislation could also address the responsibility for informing the persons affected by such systems, while also clarifying the explainability requirements and setting specific liability and certifications regimes.
2. Sector-specific legislation in the health sector.
   The Finnish national AI strategy proposes to formulate AI ethics rules specific to the healthcare ecosystem. A 2018 study by the University of Oxford stresses the need to analyze the implementation of the GDPR in the field of health

[34] "EU guidelines on ethics in artificial intelligence: Context and implementation." n.d. European Parliament.

research, and where needed, amend laws or create more clarity through interpretation and guidance.

3. Legislation on face recognition technology.
   The use of face recognition technology (FRT) is becoming widespread across Europe and is giving rise to growing concerns. FRT is considered as processing 'biometric data' under the GDPR, and is in principle subject to strict terms and conditions of use. However, technology experts disagree on whether the GDPR framework is robust enough to address all issues created by the growing use of AI-based FRT, or whether additional legislation will be necessary to ensure EU fundamental rights are protected. Already, the adoption of national FRT legislation is being discussed in some Member States.

III. India: Current Legal Status and Future Proposals

India's legal framework on data protection and artificial intelligence (AI) is currently in a state of development, driven by the rapid digitalization of the economy and focusing more towards the importance of data privacy. Presently, it does not have a comprehensive data protection law that addresses the concerns related to deployment of AI, but developments are ongoing which could reshape the regulatory landscape. The government of India has enacted a new privacy law, the Digital Personal Data Protection Act, which addresses some of the privacy concerns in AI applications and the Global Partnership on Artificial Intelligence (GPAI) , which is One of the most critical initiatives, is the Personal Data Protection Bill (PDPB). India is one of the members of this partnership, and it aims to create a robust framework for personal data processing, closely mirroring global standards such as the General Data Protection Regulation (GDPR) of the European Union, this emphasizes key principles such as the data minimization, and the rights of individuals to access and to erase personal data.

The ongoing discussions on revisions in the PDP Bills is to address concerns of various stakeholders, civil society and industry representatives, on the other hand, It proposes the establishment of a Data Protection Authority (DPA), which eventually would oversee compliance, handle grievances and ensure enforcement of data protection laws. It will also set up a culture of data privacy and accountability among organizations which deal with handling personal information.

NITI Aayog, public policy think tank of the Government of the Republic of India, and the nodal agency with bottom-up approach has released a discussion paper[35] on AI ethics in 2020, emphasizing the need for responsible AI practices, keeping transparency, accountability, and inclusivity as the main focus for the development and deployment of AI technologies though there is a need for a cohesive framework to address the ethical challenges of AI because there are many key challenges and one of the major challenges is the implementation of existing regulations and the gap in awareness and resources, especially among small and medium enterprises (SMEs), which may struggle to comply with evolving data protection standards, additionally public awareness about data protection rights is limited and underscoring the need for educational initiatives to inform citizens about their rights under potential new laws, and another challenge is finding the right balance between fostering innovation in AI and ensuring ethical practices.

6. Recommendations

1. **Establishment of an "AI Champions Programme"**
    a. **Objective:** To foster AI adoption within healthcare institutions by establishing a culture of innovation and trust.
    b. **Program Structure:** Identify and train "AI Champions" from existing healthcare staff in each institution. These Champions will:
        i. Receive comprehensive training on AI tools and ethics.
        ii. Act as peer mentors and resources for colleagues, supporting the adoption and effective use of AI.

    This will enhance trust in AI among healthcare workers, encourage its adoption, and mitigate resistance due to lack of familiarity.

2. **Public Awareness and Education Initiatives**
    a. **Public Awareness Campaigns:** Launch campaigns and AI Boot Camps tailored to healthcare professionals and the general public to build awareness about AI's role in healthcare.
    b. **Informed Consent and Data Usage Transparency:** Ensure that patients are informed about how AI is used in their treatments and data handling. Transparent policies should support patients' rights to know and consent.

[35] Kelley, Kevin. n.d. "National Strategy for Artificial Intelligence." NITI Aayog.

c. **Boot Camps for Healthcare Professionals:** Offer short-term boot camps to train doctors, nurses, and other staff on AI applications. This would boost their confidence, reduce apprehension, and enhance understanding of AI's capabilities and limitations.

3. Strengthening Data Privacy and Cybersecurity Regulations

a. **National Health Data Repository:** Establish a centralized health data repository that utilizes robust data privacy regulations with blockchain and controlled access systems.
b. **Blockchain for Data Security:** Employ blockchain for secure, immutable storage and controlled access to health data.
c. **Data Privacy Regulations:** Formulate stringent policies for the protection of patient data, addressing concerns around unauthorized access and misuse.
d. **Enhanced Cybersecurity:** Prioritize cybersecurity with AI-enabled applications to counter threats such as data breaches and cyberattacks.
e. **Automated Monitoring Systems:** Implement AI-based monitoring systems that proactively identify and respond to vulnerabilities.
f. **Incident Response Plans:** Invest in cybersecurity infrastructure and workforce training to develop comprehensive response plans for data breach incidents.

4. Regular Updates to Address Algorithmic Biases

a. **Regular Algorithm Audits:** Conduct frequent audits to identify and address biases in AI algorithms, ensuring fair and unbiased outcomes for all demographic groups.
b. **Inclusive Training Datasets:** Develop guidelines to ensure AI systems are trained on datasets representing India's diverse population to improve reliability and fairness.
c. **Community Engagement:** Encourage inputs from diverse community stakeholders in algorithm development and deployment, fostering inclusivity.

5. Development of India-Specific AI Models

a. **Localized AI Models:** Invest in research and development to create AI models specifically trained on and suited for India's population and healthcare challenges.
b. **Collaborative Research Efforts:** Establish collaborations with local academic institutions, technology firms, and healthcare providers to refine AI models based on India-specific health concerns and demographic nuances.

6. Policy Framework and Governance

a. **Establish a National AI Health Council:** Create a council comprising healthcare professionals, AI experts, policymakers, and legal experts to oversee AI deployment in healthcare, focusing on ethical and operational standards.

b. **Guidelines for AI Development and Usage:** Develop and enforce guidelines on ethical AI use, patient privacy, transparency, and inclusivity in AI-driven healthcare applications.
c. **Continuous Skill Development Programs:** Ensure ongoing training programs for healthcare workers to keep pace with AI advancements and adapt to evolving technologies in healthcare.

7. Conclusion

After in-depth analysis, it concludes that the evolution of Artificial Intelligence (AI) in healthcare is playing a vital role in modernization of the health sector, with some challenges which need to be entered through a robust uniform regulatory framework. AI has potential to diagnose and detect disease at its very initial stage. This research has discussed the global perspectives in AI integration such as the US adopting FDA guidelines as a regulatory framework for medical devices and the EU has adopted GDPR which emphasizes privacy and data protection laws. At present India's legal framework is at developing stage with Digital Personal Data Protection Act (DPDP) and ongoing discussions on ethical AI practices.

Addressing challenges related to data privacy, ethical usage, liability, and algorithmic bias has become increasingly challenging. In this phase of AI innovation, a uniform regulatory framework has become the main focus for every other country with equitable healthcare outcomes.

7. Reference

1. "EU guidelines on ethics in artificial intelligence: Context and implementation." n.d. European Parliament. Accessed October 7, 2024. https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf.
2. "Overview of Device Regulation." n.d. FDA. Accessed October 7, 2024. https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/overview-device-regulation.
3. Enikeev, Dmitry. 2022. "Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?" NCBI. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8963864/.
4. "Legal implications of artificial intelligence in health care." n.d. https://www.sciencedirect.com/science/article/abs/pii/S0738081X24000981.

5. “How an M.L.S. Prepares You for the Legal Implications of AI in Healthcare.” 2024. University of Miami News. https://news.miami.edu/law/stories/2024/05/how-an-mls-prepares-you-for-the-legal-implications-of-ai-in-healthcare.html.
6. “Cautions and Legal Considerations of Using Generative AI in Healthcare.” 2023. https://www.lexisnexis.com/community/insights/legal/practical-guidance-journal/b/pa/posts/cautions-and-legal-considerations-of-using-generative-ai-in-healthcare?srsltid=AfmBOopRFuYAcQyQpwF1eQRlUeOp9HdKoPE7lICBIIjIit2VsRh_76XP.
7. “Legal concerns in health-related artificial intelligence: a scoping review protocol - Systematic Reviews.” 2022. Systematic Reviews. https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/s13643-022-01939-y.
8. Southwick, Ron. 2024. “Hospitals and AI: Legal questions, liability and consent.” Chief Healthcare Executive. https://www.chiefhealthcareexecutive.com/view/hospitals-and-ai-legal-questions-liability-and-consent.
9. “Artificial Intelligence and Technology in Health Care: Overview and Possible Legal Implications.” 2020. Digital Commons@DePaul. https://via.library.depaul.edu/cgi/viewcontent.cgi?article=1382&context=jhcl.
10. “Obstacles to healthcare AI: legal issues relating to the increasing use of AI in healthcare and medical technologies.” 2023. International Bar Association. https://www.ibanet.org/Obstacles-healthcare-ai.
11. Hilliard, Airlie. 2024. “The State of Healthcare AI Regulations in the US.” Holistic AI. https://www.holisticai.com/blog/healthcare-laws-us.
12. “Evolving Intellectual Property Landscape for AI-Driven Innovations in the Biomedical Sector: Opportunities in Stable IP Regime for Shared Success.” n.d. Frontiers. Accessed October 8, 2024. https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2024.1372161/full.
13. “How the challenge of regulating AI in healthcare is escalating.” n.d. EY. Accessed October 8, 2024. https://www.ey.com/en_gl/insights/law/how-the-challenge-of-regulating-ai-in-healthcare-is-escalating.
14. “Policy Brief Understanding Liability Risk from Healthcare AI.” 2024. Stanford HAI. https://hai.stanford.edu/policy-brief-understanding-liability-risk-healthcare-ai.
15. Southwick, Ron. 2024. “Hospitals and AI: Legal questions, liability and consent.” Chief Healthcare Executive. https://www.chiefhealthcareexecutive.com/view/hospitals-and-ai-legal-questions-liability-and-consent.

16. “Author Post: Ethical AI in Healthcare: A Focus on Responsibility, Trust, and Safety.” 2024. Forbes. https://www.forbes.com/sites/forbesbooksauthors/2024/01/04/ethical-ai-in-healthcare-a-focus-on-responsibility-trust-and-safety/.
17. Payne, Daniel. 2024. “Who pays when AI steers your doctor wrong?” Politico. https://www.politico.com/news/2024/03/24/who-pays-when-your-doctors-ai-goes-rogue-00148447.
18. Chin, Caitlin. 2024. “Protecting Data Privacy as a Baseline for Responsible AI.” CSIS. https://www.csis.org/analysis/protecting-data-privacy-baseline-responsible-ai.
19. “The Ethics of AI in Healthcare.” 2023. HITRUST. https://hitrustalliance.net/blog/the-ethics-of-ai-in-healthcare.
20. Chin, Caitlin. 2024. “Protecting Data Privacy as a Baseline for Responsible AI.” CSIS. https://www.csis.org/analysis/protecting-data-privacy-baseline-responsible-ai.