# LEGAL AND ETHICAL CHALLENGES OF ARTIFICIAL INTELLIGENCE-DRIVEN HEALTHCARE

**By**
**Umenwa Ugochukwu**
**Minnesota State University**
**Mankato, Minnesota**
**USA**

## ABSTRACT

*Artificial intelligence (AI) is perceived to be at the forefront of the transformative era in healthcare as it offers unprecedented development in diagnostic accuracy, treatments that are personalized and high level of efficiency in operations. By brining together lots of datasets and algorithms that are sophisticated, AI-driven tools are enabling the health care providers to deliver more precise, effective and timely care. It is noteworthy that AI integration into the system of healthcare are not without its challenges. AI use raises ethical and legal issues most especially when it has to do with patient privacy, security of data and the sufficiency of the existing legal frameworks for addressing these issues. As the system of AI requires an access to personal health information that are highly sensitive to function well, this poses risks that are related to breaching of data and access that is not authorized. More so, the high probability of bias in AI algorithm may actually lead to outcomes that are neither fair nor accurate as this further complicates ethical considerations. This research work looks into ethical and legal challenges of AI-driven health care. The descriptive results of the study have shown that AI has contributed largely to the improvement in the health sector going by the metrics of life expectancy and under five mortality rate. The cases of United State of America and Europe were compared. The article provides strategies that include putting in place trustworthy cybersecurity procedures such as multi-factor authentication, encryption, and security audits carried out on a regular basis.*

**KEYWORDS: Legal And Ethical Challenges, Artificial Intelligence-Driven Healthcare**

## INTRODUCTION

The incorporation of AI into the system of healthcare is enabling the realisation of a variety of benefits that were previously unattainable, thereby facilitating a paradigm shift in the deliverance of medical services. Healthcare providers can improve patient outcomes by providing more precise diagnoses, personalised treatment plans, and more efficient decision-making processes through the use of AI technologies that often includes machine learning algorithms, natural language processing, and predictive analytics. AI facilitates the analysis of vast quantities of data, thereby reducing healthcare costs, by enabling the early detection of disease, the more precise prediction of patient outcomes, and the optimisation of resource allocation. (Abbasi, 2024b). Furthermore, AI-powered tools can streamline administrative responsibilities, affording healthcare professionals a focus more on caring for patients. However, AI integration into the system of healthcare is not without significant challenges. AI in healthcare has safety as one of its obstacles. IBM Watson dedicated to Oncology is considered one good example (IBM, 2020). To assist patients and physicians investigate different treatment of cancers, it makes use of th algorithm of AI for evaluaton of data that is from the medical rcords of patients. It was recently faced with criticism for the proposition of 'unsafe and incorrect' treatment of cancer (Brown, 2018;

Ross & Swetlitz, 2018). Watson for Oncologoy's algorithm was developed using a small number of "synthetic" cancer cases, or examples provided by physicians at the Memorial Sloan Kettering (MSK) Centre for Cancer, rather than utilising real patient data (Ross & Swetlitz, 2018). Since MSK has maintained that mistakes often occur during the system testing phase, no actual patient has ever gotten medicine that was prescribed incorrectly (Ross & Swetlitz, 2018). Field reputation has been harmed by his real incidence. It also plays an emphasis on how critical it is that Ais is secure and efficient. More so, how one can possibly make the Ais fulfil their promises? Stakeholders, most especially the developers of AI need to ensure two key and important components for the purpose of making use of AI in an effective manner. (1) the validity and datasets dependability and (2) transparency. Above all, there is a need for the datasets to be trustworthy and genuine (Gerke et al., 2020). In AI, the adage "garbage in, garbage out" is applicable. The quality oof data employed in training, often referred to as labelled data, will promote the AI's performance (Figure Eight, 2020). Additional tweaks are often needed for the algorithms to provide trustworthy findings. Data sharing is another major issue: in situations where a high level of confidence is required from AI, like cars that are self-driving, massive amounts of data—and hence rising data transmission—will be required (Figure Eight, 2020). A text-based AI with less sentiment, for instnce, may need less data in certain circumstances (Figure Eight, 2020). Generally, the volume of data that is needed highly depends on the nature of AI and the assigned task to it. Also, a certain level of openness must be guaranteed for the sake of trust and safety of the patiets. If all data and algorithms were made publicly available, it would be great, even if there are valid worries regarding safeguarding intellectual property, investments and avoiding an increase in cybersecurity risk. A solution might be offered by government or third-party audits (Gerke et al., 2020).
Additionally, any software defects (such bias in the data) and the kind of data utilized by AI developers must be revealed. Cases such as Watson for Oncology, where IBM did conceal its harmful and inaccurate treatment recommendations for more than a year, should cause concern. Finally, openness fosters trust among all parties involved, particularly between doctors and patients, which is essential for the effective use of AI in healthcare settings. The idea of creating "black-box" AI systems has disadvantages as well. It might be difficult to determine how to promote openness in certain circumstances. Even if the model were reduced to a more straightforward mathematical link between symptoms and diagnosis, the process may still include little changes that are hard for physicians and patients to fully understand. The safety and effectiveness of the AI are often confirmed by results that is positive from randomized trials other method of testing methods, so there's no need to completely "open the black box."

## UNDERSTANDING “ARTIFICIAL INTELLIGENCE”

According to scholarly study and court papers, the term "artificial intelligence" (AI), while extensively used in society, does not have a commonly recognized definition. In this instance, we shall choose a few subcategories rather than depending on a single definition. The approach that s usually being employed in AI applications that are contemporary is machine learning (ML), a branch of artificial intelligence (AI). If computational systems learn from data, they could function better without explicit programming (Mehta & Devarakonda, 2018). Multi-layered artificial neural networks are employed in the "deep learning" branch of machine learning to find patterns in big datasets (Mehta & Devarakonda, 2018).

As we will see below, the most significant ethical and legal problems arise when machine learning algorithms are more akin to "black boxes"—that is, when the outcomes are very difficult for physicians to fully comprehend (Mehta & Devarakonda, 2018).

## TRENDS AND STRATEGIES

This section's primary emphasis is on US and European AI policies and their approaches to compete with China, the industry's biggest opponent. This carries on the discussion of the moral and legal concerns surrounding AI in research and healthcare. We'll look at recent advancements in the field and discuss a number of AI solutions that are now being used in US and European healthcare settings.

## UNITED STATES

In addition to AI applications for the public good, US Government reports on the topic during Barack Obama's presidency concentrated on safety, justice, and governance concerns (US Government, 2016, “Preparing for the Future of Artificial Intelligence,” pp. 13, 14, and 3034; US Government, 2016, “The National Artificial Intelligence Research and Development Strategic Plan” and “Artificial Intelligence, Automation, and the Economy,” among others). One of the papers highlighted the need of improving justice, accountability, and transparency by design in addition to developing ethical AI (US Government, 2016, “The National Artificial Intelligence Research and Development Strategic Plan,”).

Since Donald trump assumed office more than five years ago, the AI policy of US has shifted towards a market approach known as free market (Dutton, 2018). For example, AI was hosted by the white house on industry Summit in USA in May 2018. Among the important takeaways from the breakouts of the summit sessions was that Administration of the Trump wanted to do away with regulatory barriers to the development of AI (White House, 2018), “Summary of the white house summit in 2018 on Artificial intelligence for American industry). One of the administration’s top R&D investment goals for the year 2020, based on the announcement on July 2018 from the Executive Office of the president (Executive Office of the President, 2018). The executive order was issued by Trump for maintaining Leadership in America in Artificial Intelligence” in February 2019 which is in response to claims that the US has taken a more permissive approach to AI than other countries, China most especially (White House, 2019). The initiative of American AI is a coordinated endeavour of the federal government which was known to have been created by Trump order. This focus on five important areas that include funding for AI research and development, Ai resource supply, educating the AI workforce, AI governance policies, maintaining the competitiveness in AI and international affairs (White House, "Accelerating America's Leadership in Artificial Intelligence" Executive Order, 2019).

In 2020 January, AI recommendations for regulations was released by the white House (Whiet House, 2020), ‘Heads of Executive Departments and Agencies Draf Memorandum for the : guidance for AI regulation include public participation, public confidence in Artificial Intelligence, adaptability, nondiscrimination and equality, safety and security, openness and transparency, scientific integrity and equality of information, assessment of risk and information equality, and benefits, and interagency collaboration. The white house in February 2020, also makes a publication of yearly report on the initiative of American that is capable of summarizing the

progress that has been made since the executive order was signed by Trump OECD, 2019). The OECD principles of AI, which has the aim of creating reliable AI while also respecting democratic ideals and human rights, were adopted by more than 40 nations in May 2019. This write shows how the United States had had key role in the course of developing these concepts (White House, 2020); G20, G20 ministerial statement on Digital and trade economy. Anew website that is called 'AI.gov' White House which focuses on AI for the people in America to make provision for American platform to have more knowledge on AI and as well as its potential. Since Trump assumed office on January 20, 2017, quite a number of AI related measures were submitted in the US congress, in which Future of AI Act is included (S.2217 and H.R.4625 ), the act of AI jobs of 2019 (H.R.827), and also act for self-drive (H.R.3388). The self-drive Act seems the only to pass one chamber (the US chamber of representatives), but there is none of these plans really address both the moral and legal ramifications of AI in the system of healthcare. For instance, the FUTURE two bills of AI Act of the year 2017 tend to demand that the secretary of commerce for creating federal advisory board for the provision of advice to the secretary under sections (b)(1) and 4(a). This community will evaluate among other things, the way ethical standards may be applied to the development and use of AI [Sec. 4(b)(2)(E) or how the AI advancement might impact the reduction of healthcare costs [Sec. 4(b)(2)(L)]. More so, state and local AI related legislation is being draughted (FLI Team, 2019). For example, the 23 Asilomar AL principles were legally adopted by the State of Califonia in August 2018 when legislation (ACR-215) was approved (FLI Team, 2019; FLI team, 2018).

In health care settings, AI is being used in the United States. AI is promising, most especially, in the domain of diagnostics and imaging.

IDx Technologies Inc. (2018) and the FDA (2018) An artificial intelligence (AI) gadget that can identify specific diabetic eye diseases has been cleared for sale by the FDA. IDx/DR, the first approved FDA AI diagnostic tool, determines the screening result without the need for picture interpretation or human input. To detect adults with diabetes (age 22 and up) who have more than a mild form of diabetic retinopathy, the FDA authorised the marketing of this device that is AI-based in April 2018 (FDA, 2018, DeNovo Summary DEN180001). Suppose the IDx-DR software detects more than moderate diabetic retinopathy. In that case, it suggests that the patient consult an eye specialist or undergo another test within a year (FDA, 2018 FDA Permits Marketing of Device that is AI-Based to Detect Certain Diabetes-Related Eye Problems. The doctor will upload the retinal pictures of the patient to a cloud server. To help clinicians detect distal radius fractures, a common type of wrist fracture in adult patients, the FDA also approved the marketing of Imagen's OsteoDetect software in May 2018 (FDA, 2018).

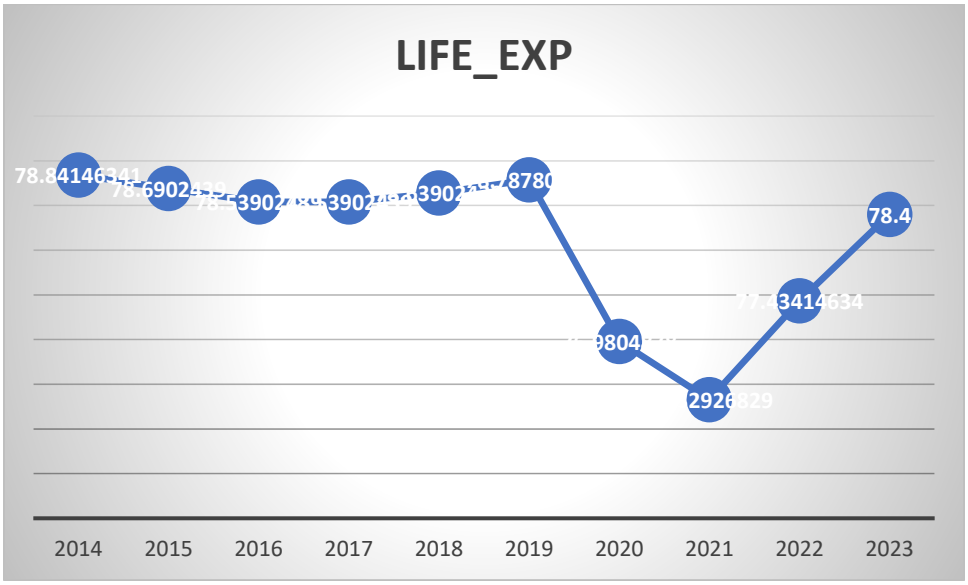
## METRICS FOR HEALTHCARE PERFORMANCE

The data below shows life expectancy, death rate and under-five mortality rate from 2014 to 2023.

In recent years, the United States has experienced significant advancements in AI and robotics, driven by major developments in machine learning, automation, and data analytics. According to a report from Stanford's Institute for Human-Centered AI (Lam, 2024), there has been more than a 50% increase since 2020 in the implementation of AI across industries including healthcare, finance, and manufacturing. In these sectors, robotics have become essential for boosting efficiency and reducing costs. Moreover, the U.S. federal government is actively fostering growth in AI through initiatives like the National AI Initiative Act of 2020 that aim to preserve global leadership in this domain (Chandra, 2020).

| Country Name | YEAR | LIFE_EXP | Death_rate | UMR |
|---|---|---|---|---|
| United States | 2014 | 78.84146 | 8.237 | 7.5 |
| United States | 2015 | 78.69024 | 8.44 | 7.4 |
| United States | 2016 | 78.53902 | 8.493 | 7.3 |
| United States | 2017 | 78.53902 | 8.638 | 7.2 |
| United States | 2018 | 78.63902 | 8.678 | 7.2 |
| United States | 2019 | 78.7878 | 8.697 | 7.1 |
| United States | 2020 | 76.98049 | 10.27 | 6.9 |
| United States | 2021 | 76.32927 | 10.4 | 6.8 |
| United States | 2022 | 77.43415 | 9.8 | 6.7 |
| United States | 2023 | 78.4 | 8.66 | 5.15 |

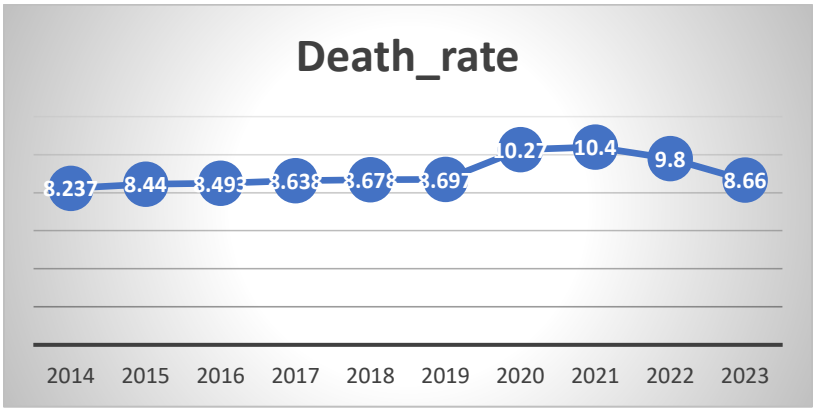
Source: WDI, 2025




Source: Author, 2025

Figure 1: Life expectancy

The figure 1 shows that health sector performance has been increasing since 2020, the year when AI and robotics were mentioned to have boomed by more than 50%. It can therefore be inferred from the figure that AI and Robotics have contributed immensely to the healthcare.




Source: Author, 2025

Figure 2: The Death Rate after 2021 has been shown to have been reducing, as this points to the likelihood that the proliferation of both Robotics and AI might have led to a large reduction in death rate in USA.

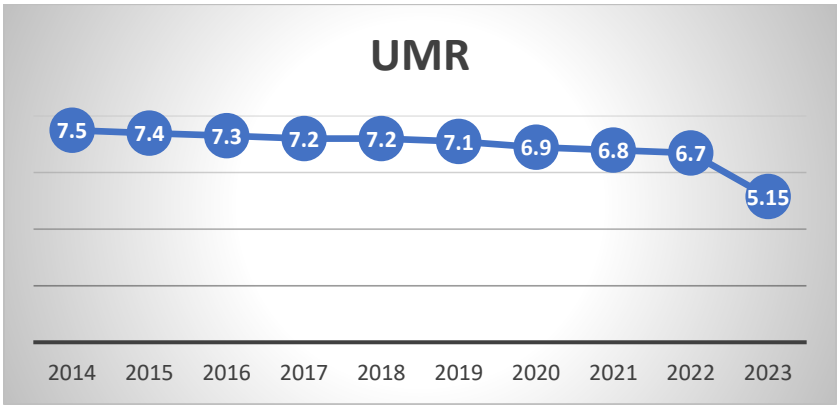



Figure 3: Under Five Mortality Rate

Also, figure 3 shows a drop in the rate of under five mortality rate which also points to the huge contribution of both Robotics and AI in the reduction of mortality rate under five in the US from 2020 through 2023.

**Europe**

As suggested in the previous section, AI use in the clinical healthcare practice tends to have a huge potential for transforming it for the better, however, it raises some ethical challenges this section tends to address.

**Informed consent Prior usage**

The health AI application can alter Patient-physician interactions in imaging, diagnostic and in surgery. However, how can informed consent and AI-assisted patient care coexist? Despite the fact that informed consent is a critical issue which has not received adequate focus in the ethical debate, it will be one of the most significant obstacles to the AI integration into clinical practice (Cohen et al., 2014). It is essential to evaluate whether the informed consent criterion should be implemented when employing therapeutic AI. What is the extent to which physicians are obligated

to inform patients about the intricacies of artificial intelligence, like the machine learning (ML) the system employs, the data it accumulates, and the potential for biases data defects it uses? When is it permissible for a physician to discuss artificial intelligence with a patient?

**Safety and transparency**

The implementation of AI in the system of healthcare is significantly impeded by safety concerns. IBM Watson for Oncology is another well-known example of this (IBM, 2020). It employs artificial intelligence algorithms for data analysis from patient medical documents in order to assist physicians and patients in making decisions regarding cancer therapy. The concept of "unsafe and incorrect" alternatives to cancer therapy has recently been the subject of debate (Ross & Swetlitz, 2018). The training provided by Watson for Oncology is the apparent issue, as per Ross and Swetlitz (2018). Instead of actual data of patient, the program was trained using a limited number of "synthetic" cancer cases that were generated by clinicians at the Cancer Centre of Memorial Sloan Kettering. MSK maintains that errors have only happened in the course of system testing; as a result, no actual patient has ever received inaccurate treatment recommendations (Ross & trewetlitz, 2018).

The reputation of the field has been adversely affected by this incident. It also underscores the importance of AIs being both efficient and secure. Nevertheless, how can we ensure that AIs fulfil their responsibilities? In order to effectively implement AI, stakeholders, particularly AI developers, must guarantee the validity and veracity of transparency and datasets. The datasets has to be authentic and reliable above all else. The adage "garbage in, garbage out" is pertinent in the field of AI. The AI will exhibit superior performance when it is provided with superior training data (labelled data) (Figure Eight, 2020). In order to achieve consistent outcomes, algorithms frequently necessitate additional refinement. Another substantial issue is the exchange of data. In scenarios where the AI must exhibit a high level of confidence, such as self-driving automobiles (Figure Eight, 2020), a substantial amount of data—and subsequently, an increased rate of data sharing—will be necessary. Conversely, certain scenarios necessitate less information, such as emotion AI that is text-based (Figure Eight, 2020). The quantity of data necessary is typically determined by the form of AI and its capabilities.

**Algorithmic biases and fairness**

In addition to the potential to democratise information and "globalise" healthcare, Wahl et al. (2018) assert that AI has the potential of improving healthcare in both affluent and rural populations. Nevertheless, the quality data meant for training has a substantial effect on the efficacy, reliability and equity of any algorithm or system of machine learning that is instructed by humans. Prejudice and discrimination are equally susceptible to AI. AI developers must be aware of this peril and strive to mitigate any potential biases throughout the entire process of developing new products. When selecting (1) the datasets to be used for programming and (2) the machine learning techniques or resources to train the algorithms, bias risk should be meticulously assessed. This encompasses quality and diversity considerations. There is an abundance of real-world examples that illustrate how algorithms may show biases that is capable of resulting in injustice based on skin pigmentation, skin complexion, or gender (Sharkey, 2018). Biases against some other features, such as disability and age, may also exist. These biases are the result of a variety of

complex factors. They may be derived from non-representative datasets, the artificial intelligence ecosystem, algorithms of machine learning that select and assess data (Price II, 2019). For example, the safety of medications used in the medical field may be jeopardised by biassed AI, which can lead to inaccurate diagnoses which can undermines the effectiveness of treatments for specific subpopulations when phenotype--and frequently genotype--related data is included. A clinical decision support instrument that employs AI to aid physicians in making the most appropriate decisions for patients with cutaneous cancer is currently under consideration. Provided there the algorithm was mainly trained based on Caucasian patients, it may provide recommendations that are less reliable or even inaccurate for under-represented subpopulations, such as African Americans. By enhancing data accessibility, providing more detailed descriptions of which populations the algorithm is or is not appropriate for, and making an effort to acquire data from minority groups in a trustworthy manner, many of these biases may be mitigated. Nevertheless, the complexity and opacity of a plethora of algorithms persist as a source of concern. Furthermore, the claim that their work is classified as a trade secret is made by certain software development companies, which has been observed in the context of policing (Sharkey, 2018; Wexler, 2018). Consequently, nonprofit organisations may be able to collect data and disclose these biases.

**DATA PRIVACY**

The NHS Royal Free Foundation Trust was established to have violated the Data Protection Act 1998 of the UK in July 2017 by disclosing roughly 1.6 million patients' personal data to Google DeepMind (Powles & Hodson, 2017; Wachter, Mittelstadt, & Floridi, 2017). The primary focus of data sharing for clinical safety evaluations was "Streams," an application that enables the monitoring and identification of acute renal failure (Wachter et al., 2017). Nevertheless, no sufficient information to the patients regarding how their data would be utilised by the test (Wachter et al., 2017). It was correctly observed by Elizabeth Denham, the Information Commissioner, that the neglect of privacy rights that are fundamenta is not an inevitable consequence of innovation (Wachter et al., 2017). Despite the absence of artificial intelligence in the Streams app, this real-world example has heightened awareness of the potential for privacy rights which is to be violated in the course of the development of technological solutions (Cohen, 2019). In the end, the AI integration into clinical practice successfully will be rendered ineffective if physicians and patients lack confidence in it. It is essential to establish open communication and afford patients with sufficient information on the use of their data in order to establish their trust. The focus has shifted to patient privacy concerns regarding data sharing and AI use in recent case studies, including Ascension (Ross & Swetlitz, 2019), Google's Project Nightingale, and Dinerstein v. Google (Wagner, 2020). However, what is the current status of data ownership? There is evidence that the public is apprehensive about governments or corporations selling patient information for profit, despite the potential data value on health in billions USD (Cohen, 2019). Nevertheless, patients have the capacity to convey their appreciation in alternative manners excluding ownership. For an instance, the NHS Royal free Foundation Trust consented to furnish Google DeepMind with patient data designed for testing Streams in exchange for five years of complimentary app usage (Cohen, 2019). Reciprocity may not require ownership; however, all parties who intend to utilise patient data must exhibit their involvement.

**EFFECTIVENESS AND SAFETY**

It is imperative that AIs continue to be effective and safe. Stakeholders may contribute to the effective use of AI the practice of clinical health, by ensuring that the datasets are reliable and genuine, upgrading software often, and being forthright about the shortcomings of their product, including data biases. Furthermore, appropriate legislation is needed to ensure AI's effectiveness and security. This is not the situation in the Europe and US. So, how is AI regulated in the US and Europe? How can businesses advertise their products in the US and Europe using artificial intelligence? Assessing whether AI products are medical devices is the first step in deciding if they need review.

**United States**

Starting with the legal regulation in the US.

**Medical devices**

The FDA is responsible for the enforcement of US laws that pertain to medical equipment. A medical device is understood to be "any instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is 1. recognised in the United States Pharmacopoeia, the official National Formulary, or any supplement to them; 2. intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals; or 3. intended to affect the structure or any function of the body of man or other animals; and which does not rely on chemical action within or on the body of man or other animals to achieve its primary intended purposes," in accordance with FDCA Section 201(h).

**Software for Medical and Specific Decision Support**

On December 13, 2016, the Cures Act 21st Century (Pub. L. No. 114–255) got signed into law by Barack Obama, former US president. At first, there was a sense of optimism that the FDA would regulate Watson for Oncology and other medical advising systems in a manner that was suitable (Ross and Swetlitz, 2017). However, IBM maintains an extensive lobbying team that is dedicated to the circumvention of regulations related to health software (Ross and Swetlitz, 2017). IBM promised to "continue to advance precision medicine and promote health innovation in the United States" in a press statement on 29th of November, 2016, the day prior to hen the US House of Representatives approved the 21st Century Cures Act (Ross & Swetlitz, 2017; IBM, 2016). FDCA Section 520(o) does not apply to medical and specialised decision support software that does not meet the device standards specified in Section 3060 of the 21st Century Cures Act. Furthermore, the FDCA of Section 201(h) was amended to include a second paragraph that forbids software activities covered by Section 520(o) of the FDCA from being categorised as "devices."

**Privacy and Data Protection**

In the era of big data, it is essential that laws on data protection exist that adequately protect people's privacy, especially that of patients. Health data security is a primary concern in the digital era of healthcare that is AI-driven, as a significant amount of sensitive patient information is collected, processed, and retained by a variety of digital systems. The AI integration into the system of healthcare further exacerbates these concerns, as AI systems frequently require extensive

datasets, including confidential health information (PHI), to function as intended. A compromise of this data has the potential to result in severe consequences, including financial loss, identity deception, and a loss of patient trust. As a result, it is imperative to guarantee its security.

Below is a summary of relevant legislation and legal developments concerning data protection and privacy in the US and Europe.

**United States**

The Portability of Accountability Act and Health Insurance (HIPAA) Privacy Rule (45 C) is the primary federal statute that safeguards the privacy of health data (Price II & Cohen, 2019). Despite offering unique security for some health information produced by "covered entities" or their "business associates," HIPAA has a number of shortcomings that significantly affect the contemporary healthcare system. One example of nonhealth data that supports medical outcomes and is not subject to HIPAA laws is the purchase of a pregnancy test on Amazon (Cohen, 2019; Cohen & Mello, 2018).

Its reach is further limited by the term "covered entities," which include insurance carriers, insurance services, insurance clearinghouses, insurance organisations, and healthcare providers in general (45). But a lot of other information is omitted (Price II & Cohen, 2019Cohen & Mello, 2018, ; ). In particular, a significant portion of health data collected by digital behemoths like Amazon, Google, IBM, Facebook, and Apple—which are not "covered entities" but are making significant investments in the use of artificial intelligence in healthcare—will not be subject to HIPAA restrictions (Price II & Cohen, 2019). Furthermore, HIPAA is not applicable to health information generated by users (Price II & Cohen, 2019; Cohen & Mello, 2018). For instance, Cohen and Mello (2018) noted that a Facebook post on a sickness is exempt from HIPAA.

**Europe**

"Data concerning health" as the GDPR defines it. In the healthcare industry, Article 4(15)—"personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status"—is especially pertinent. The GDPR in the HIPAA and EU in the US vary greatly from one another. The former concentrates on particular health information generated by "business associates" or "covered entities" (Cohen & Mello, 2018). Certain forms of personal data, like genetic data (Article 4(13) of the GDPR), biometric data (Article 4(14) of the GDPR), and health data, are prohibited from processing under Article 9(1) of the GDPR. Nonetheless, Article 9(2) of the GDPR has a list of exceptions to paragraph 1 (Gerke et al., 2020). The GDPR is generally exempt from Article 9(1) in the following situations, according to Cohen and Mello (2018) and Gerke et al. (2020): "processing is necessary for reasons of public interest in the area of public health," "the data subject has given explicit consent (...) for one or more specified purposes," or even "for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes."
" A corporation that breaches specific GDPR duties may face administrative penalties of up to 20 million EUR, or 4% of its yearly worldwide sales from the prior year, if higher, in accordance with GDPR Article 83(5). The GDPR has already resulted in the first fines in the healthcare industry. For instance, a Portuguese hospital allowed professionals to "indiscriminately access a set of data

by professionals, who should only be able to access them in specific cases" and failed to "ensure the confidentiality, integrity, availability and permanent resilience of treatment systems and services" ([European Commission], 2020). The hospital was therefore fined 400k euros for breaking two GDPR regulations.

The GDPR's Article 4(15) definition of "data concerning health"—"personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status"—is especially relevant to the healthcare sector. For health data created by "covered entities" or their "business associates," which is all that HIPAA protects, the GDPR in the EU provides further protection.

**Cybersecurity**

Cybersecurity is another important consideration when talking about legal issues related to AI use in healthcare system. In the future, a large percentage of products of healthcare, services, and operations will operate inside the Internet of Things. Regretfully, both physical and cyberattacks may affect a significant portion of the auxiliary infrastructure (US Department of Homeland Security, 2019). To steal or change the flow of money or important (healthcare) data, for example, nation-states, criminals, and competent cyber actors may exploit vulnerabilities (US Department of Homeland Security, 2019). The ability of these actors to jeopardise, harm, or obstruct the delivery of essential (medical) services is growing (US Department of Homeland Security, 2019). Hospital servers, wearable technology, medical equipment, diagnostic tools, and wireless smart drugs are a few possible goals for the healthcare industry (Pinsent Masons, 2017). All of them are vulnerable to software attacks, Trojan horses, and worms that jeopardise patient privacy and health (Pinsent Masons, 2017). Additionally, inaccurate and harmful treatment recommendations might be the consequence of biassed data or tainted algorithms (Gerke et al., 2020). Hostile actors may compromise patient safety and get private information, including medical data, by fabricating medical records. Finlayson et al. (2019) assert that artificial intelligence is especially susceptible to manipulation. The "WannaCry" ransomware attack, which used advanced hacking tools to infect over 300,000 computers in 150 countries (Graham, 2017). To accurately classify a mole as malignant, for example, a little modification in inputs may have a significant impact on the system's output (Finlayson et al., 2019). A little modification to the system's inputs might result in a completely different output, claim Finlayson et al. (2019). According to Gerke, Kramer, and Cohen (2019), the method may thus be 100% accurate in classifying a mole as malignant.

**Strategies to Strengthen Health Data Security**

To tackle these challenges, healthcare organisations need to develop a thorough health data security strategy. This entails putting in place trustworthy cybersecurity procedures including encryption, multi-factor authentication, and frequent security audits. Because encryption ensures that data cannot be easily accessed or read by unauthorised people, even if it is intercepted, it is essential (Mettler, 2016). Healthcare companies should also spend money on state-of-the-art cybersecurity tools and technologies that use artificial intelligence (AI) and machine learning to quickly detect and eliminate threats. For instance, AI-powered security systems may monitor network traffic for unusual patterns that could point to an attack, reducing the likelihood of harm and enabling faster response times (Nizamullah et al., 2024). Another important strategy is the establishment of a security culture inside healthcare organisations. Employees in the healthcare industry get training on the best data security procedures, such as how to recognise phishing attempts and manage private information properly. Employee education may significantly lower

the risk of data breaches, which are often the result of human error (Alotaibi & Federico, 2017).

Healthcare organisations must also periodically evaluate and modify their data protection policies to ensure that they comply with relevant legislation. This entails conducting risk assessments to identify any vulnerabilities and implementing mitigation techniques. Organisations must keep abreast of regulatory developments in addition to ensuring ongoing compliance and avoiding legal repercussions. In conclusion, enhancing data security requires the collaboration of healthcare professionals. By exchanging information about hazards and best practices, organisations may keep informed about new threats. Public-private partnerships, which include government agencies collaborating with private companies to enhance cybersecurity, may also help secure health data (Esfahani, 2024). Health data security is a big concern in the era of artificial intelligence (AI) in healthcare, and safeguarding private patient information is essential. While there are numerous benefits to the increasing usage of AI systems, there are also new security risks that must be addressed. Establishing a security culture within healthcare organisations, implementing comprehensive cybersecurity measures, and ensuring that rules are followed may all help to lessen the risks associated with the protection of health data. To ensure that the benefits of AI in healthcare are realised without endangering patient privacy or trust, the techniques used to protect health data must also evolve as AI does.

**CONCLUSION**

This chapter focused on the legal and ethical controversy surrounding AI in healthcare system and research by providing an overview of the technology and discussing trends and tactics in the Europe and US. The amount of AI products that have already made their way into the US market, including the first FDA-approved autonomous AI diagnostic system, IDx-DR, indicates that the US has a more open market policy than Europe. According to one estimate, artificial intelligence (AI) might boost the world economy by up to 13.33 trillion euros by 2030. China, North America, and Southern Europe would benefit the most from AI, according to the European Commission (2018). Europe, on the other hand, is becoming a worldwide leader in AI ethics.
Specifically, in 2019, April, the European Commission of the High-Level Expert Group on AI of released Guidelines on ethics for Trustworthy AI.
There is a need to resolve four main ethical issues before AI is used in healthcare: algorithmic fairness, data privacy and biases, informed consent, safety and transparency. Liability, cybersecurity, data protection and privacy, intellectual property law, and safety and effectiveness were the five legal issues that were investigated in the US and Europe. To guarantee that AI is be utilised successfully in a way that is morally and legally acceptable, it is necessary key that all stakeholders—including AI developers, healthcare providers, patients and regulatory bodies—cooperate to solve the aforementioned challenges.
The develop successfully, an AI-driven system of healthcare largely based on the ‘motto Health AIs for All of Us’ requires addressing a number of critical issues, including high levels of data, informed consent, high standards of safety, cyber resilience and cybersecurity, protection and privacy, algorithmic fairness, regulatory oversight, a sufficient degree of transparency, and effectiveness, and an ideal Ais liability regime. It is not enough to just update existing legal frameworks to take new technological advancements into account. The ethics of healthcare that is AI-driven, however, should also be the subject of serious public and political debate given its implications for human labour and society as a whole.

## REFERENCES

Abbasi, N. (2024). Artificial Intelligence in Remote Monitoring and Telemedicine. Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023, 1(1), 258–272. https://doi.org/10.60087/jaigs.v1i1.202

Arterys. https://www.arterys.com; 2019 [accessed 26/01/2025].

Brown J. IBM Watson reportedly recommended cancer treatments that were 'unsafe and incorrect'. Gizmodo, https://gizmodo.com/ibm-watson-reportedly-recommended-cancer-treatments-tha-1827868882; 2018 [accessed 26/01/2025].

Cohen IG, Amarasingham R, Shah A, Xie B, Lo B. The legal and ethical concerns that arise from using complex predictive analytics in health care. Health Aff 2014;7:113947. Available from: https://doi.org/10.1377/hlthaff.2014.0048.

FDA. FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems, https://www.fda.gov/newsevents/newsroom/press-announcements/ucm604357.htm; 2018 [accessed 26/01/2025).

Figure Eight. What is training data?, https://www.figure-eight.com/resources/whatis-training-data; 2020 [accessed 26/01/2025].

Finlayson SG, Bowers JD, Ito J, Zittrain JL, Beam AL, Kohane IS. Adversarial attacks on medical machine learning. Science 2019;363:12879. Available from: https://doi.org/10.1126/science.aaw4399.

FLI Team. State of California endorses Asilomar AI principles, https://futureoflife.org/2018/08/31/state-of-california-endorses-asilomar-ai-principles; 2018 [accessed 26/01/2025].

Gerke S, Minssen T, Yu H, Cohen IG. Ethical and legal issues of ingestible electronic sensors. Nat Electron 2019;2:32934. Available from: https://doi.org/10.1038/s41928-019-0290-6.

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial intelligence in healthcare* (pp. 295-336). Academic Press.

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial intelligence in healthcare* (pp. 295-336). Academic Press.

Graham C. NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history, https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive; 2017 [accessed 02/02/2025].

IBM. IBM letter of support for the 21st Century Cures Act, https://www.ibm.com/blogs/policy/ibm-letter-support-21st-century-cures-act; 2016 [accessed 26/01/2025].

Marr B. First FDA approval for clinical cloud-based deep learning in healthcare. Forbes. https://www.forbes.com/sites/bernardmarr/2017/01/20/first-fda-approval-for-clinical-cloud-based-deep-learning-in-healthcare/#6af107d161c8; 2017 [accessed 26/01/2025].

Mehta N, Devarakonda MV. Machine learning, natural language programming, and electronic health records: The next step in the artificial intelligence journey? J Allergy Clin Immunol 2018;141:201921. Available from: https://doi.org/10.1016/j.jaci.2018.02.025e1.

OECD. OECD principles on AI, https://www.oecd.org/going-digital/ai/principles; 2019 [accessed 26/01/2025].

Pinsent Masons. New 'digital' pills pose data protection and cybersecurity challenges for drugs manufacturers and health bodies, says expert, https://www.out-law.com/en/articles/2017/november/new-digital-pills-pose-data-protection-and-cybersecurity-challenges-for-drugs-manufacturers-and-health-bodies-says-expert; 2017 [accessed 02/02/2025].

Price II WN. Medical AI and contextual bias, Harv J Law Technol, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=53347890; forthcoming 2019 [accessed 26/01/2025].

Ross C, Swetlitz I. IBM's Watson supercomputer recommended 'unsafe and incorrect' cancer treatments, internal documents show. STAT, https://www.statnews.com/2018/07/25/ibm-watson-recommended-unsafe-incorrect-treatments; 2018 [accessed 26/01/2025].

Sharkey N. The impact of gender and race bias in AI. Humanitarian Law Policy, https://blogs.icrc.org/law-and-policy/2018/08/28/impact-gender-race-bias-ai; 2018 [accessed 08.08.19].

US Department of Homeland Security. Cybersecurity, https://www.dhs.gov/topic/cybersecurity; 2019 [accessed 02/02/2025].

Wachter S, Mittelstadt B, Russell C. Counterfactual explanations without opening the Black Box: automated decisions and the GDPR. Harv J Law Technol 2018;31:842.

Wahl B, Cossy-Gantner A, Germann S, Schwalbe NR. Artificial intelligence (AI) and global health: how can AI contribute to health in resource-poor settings? BMJ Glob Health 2018;3:e000798. Available from: https://doi.org/10.1136/bmjgh-2018000798.

White House. Draft memorandum for the Heads of Executive Departments and Agencies. Guidance for regulation of artificial intelligence applications,

https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf; 2020 [accessed 26/01/2025].