DOI: https://doij.org/10.10000/IJLSI.112303

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 6

2024

A Comparative Study of International Frameworks: Navigating the Medicolegal Challenge (Privacy) of AI Integration in Healthcare

DANUSA T.[1] AND SANTHIYA K.[2]

ABSTRACT

Artificial intelligence (AI) refers to systems or machines that imitate human cognitive functions and is able to learn from previous data and refine its performance as it goes on doing tasks. Backgrounds of informatics and computer science have brought about noticeable progress in artificial intelligence (AI) making it an essential part of today's healthcare practice. These days, artificial intelligence (AI) is applied not only to general medicine to analyse reports, but also to oncology, radiology, cardiological diseases and ophthalmology.

Artificial Intelligence using Machine Learning has supported the developed countries like the United States, China, and European nations like Germany and Italy in the medical industry. India, a developing nation that is rising decisively, is going through a major digital revolution with many startups. IBM's Watson a healthcare chatbot helps surgeons with its extensive medical expertise and data analysis skills; it is installed in hospitals in India.

The purpose of this study is to examine how developing nations with an extensive array of AI-induced medical treatments can keep on offering excellent healthcare even in the absence of a set regulatory agency to monitor the use of AI. In order to emphasize the medicolegal challenge(privacy) faced by AI in healthcare, this article compares the regulatory frameworks of AI in the US, India, and Myanmar. It also explores the gaps in regulation that still exist. This study employs a normative juridical research method with an analytical approach. The conclusion we have reached through this study is that the countries are trying to incorporate AI within their existing legislation to protect patient data privacy which is still found to be insufficient.

***Keywords**: Artificial Intelligence, Medical sector, Medicolegal, Privacy, Jurisdiction.*

[1] Author is a student at SASTRA Deemed University, India.

[2] Author is a student at SASTRA Deemed University, India.

I. Introduction

AI pioneers have created tools that improve medical research, streamline clinical care processes, and optimize healthcare delivery. In the US it was introduced in early 1970s.In the period between 1980-90s Algorithms programs were made from healthcare data that can generate predictions or recommendations, and they are the foundation of artificial intelligence-based medical devices. In the medical domain, artificial intelligence algorithms are frequently referred to as "Black-box medicine" or predictive analysis. This is due to the fact that the medical conclusions made by this machine learning thinking algorithm are not always clear-cut and may even alter over time due to the growing body of available data.

The rise in popularity of AI in the medical field has made it necessary for regulatory authorities to create rules for its use. The World Health Organisation (WHO) and the EQUATOR Network (Enhancing the Quality and Transparency of Health Research) are two organizations that have standards on the adoption of artificial intelligence in healthcare[3].

"Relating to the law concerning medical questions"[4] is the definition of medicolegal. Thus, the scope encompasses professional discipline, ethics, and law (criminal, civil, and administrative). Medical services require extreme caution since they are intricate, closely integrated systems that are always laced with danger. Laws governing AI ought to be able to assess and guarantee the precision and safety of medical judgments rendered by "thinking algorithms" in AI.

On September 17, 2024, Veyond Metaverse—a frontrunner in XR healthcare technology—completed the first-ever AI-powered 5D XR surgery[5]. Over a distance of 13,600 km, Prof. Dr. Aung Kyaw Tun conducted the surgery in Yangon, Myanmar, under the remote guidance of Prof. Dr. Thierry Flam from New York, USA. 5D XR technology improves surgical accuracy and collaboration over long distances by combining immersive 3D graphics, real-time collaboration, and AI-powered insights. In September 2023, the world witnessed its first XR digital surgery; this event represents another significant milestone.

Since AI is being used more and more everywhere in the world, including in developed and developing countries, these nations should concentrate on the evolving elements of AI from a multidisciplinary standpoint.

[3] Gary S. Collins et al., Protocol for Development of a Reporting Guideline (TRIPOD-AI) and Risk of Bias Tool (PROBAST-AI) for Diagnostic and Prognostic Prediction Model Studies Based on Artificial Intelligence, 11 BMJ Open e048008 (2021).

[4] Black's Law Dictionary.

[5] Prodigy Press Wire, Veyond Metaverse Shatters Boundaries with World's First AI-Powered 5D XR Surgery, Digital Journal (Sept. 18, 2024), https://www.digitaljournal.com/pr/news/prodigy-press-wire/veyond-metaverse-shatters-boundaries-world-s-183098544.html.

(A) Literature review

1." Emerging Artificial Intelligence In Therapeutic Agreements With A Medicolegal Approach" by Reka Dewantara and Rekyan Pandansari (2024)[6] : Medical law, sometimes known as medicolegal practice, is closely associated with the field of medicine. In this paper, a few questions were raised: How can the efficacy and security of AI thinking algorithms be guaranteed? and Is it possible to legally verify AI's accuracy and security? The study employed a statutory approach, referring to how legal studies were carried out using applicable positive legal regulations. The users of therapeutic agreements, which are the same as conventional agreements and bind the parties like statutory regulations, should be aware of the legal implications of utilizing AI as a party in e-health applications. The Policy on Privacy is a therapeutic agreement in the form of an electronic contract; in particular, there are a number of articles that outline the parties' rights and obligations that do not comply with legal requirements. The contradictory agreement's clauses must be handled carefully since they run the risk of being declared void, in which case one of the parties could petition the court to declare the agreement null and void. The safety and accuracy of medical judgments made by an AI "thinking algorithm" should be able to be assessed and ensured by the legal requirements governing AI using a medicolegal approach.

2. "Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States" by Filippo Pesappan, Caterina Volonte, and others (2017)[7] : Regulation of AI in relation to the development of medical devices and methods for ensuring the safety and utility of AI applications in the future is discussed here. They have evaluated current advancements while analysing the legislative frameworks that govern medical devices and data protection in the US and Europe. The methods used by the EU and the US for approving and regulating new medical devices differ. Cyberattacks, incidents (notification and minimization), and service continuity are all taken into account by EU laws and U.S. laws need both explicit customer agreement and opt-in data processing and use. It will be necessary to address issues like the new policy initiatives, cybersecurity and data protection regulations, the discussion of unusual accountability and responsibility issues, and the concerns about the fiduciary relationship between patients and AI medical systems as soon as possible.

[6] Reka Dewantara & Rekyan Pandansari, Emerging Artificial Intelligence in Therapeutic Agreements with a Medicolegal Approach,(2024), https://fhukum.unpatti.ac.id/jurnal/ballrev/article/view/1914/pdf.

[7] Michael Lupton, Some Ethical and Legal Consequences of the Application of Artificial Intelligence in the Field of Medicine, Semantic Scholar (2018), https://pdfs.semanticscholar.org/fd03/6646636ac9e61fc7903b0fa9fa4afebbd4f5.pdf.

3."Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?" by Nithesh Naik, B.M.Zeeshan Hameed and others (2022)[8] : The use of artificial intelligence in healthcare settings may give rise to legal and ethical difficulties that currently unresolved by established legislation. The review endeavours to tackle these significant concerns, emphasizing the necessity of algorithmic openness, privacy, and safeguarding of all the stakeholders involved, along with cybersecurity measures to mitigate related vulnerabilities. The European Parliament's Committee on Legal Affairs requested that the policy department for "Citizens' Rights and Constitutional Affairs" commission, oversee, and publish the research that served as the basis for the resolution. Evidence points to AI models' large-scale deployment and embedding of social and human biases. But the real culprit here should be the underlying data rather than the algorithm. The study highlights how urgent it is to pass a resolution mandating the immediate development of a legislative framework governing robotics and artificial intelligence that can foresee and accommodate any medium-term technological advances.

4."Revolutionizing healthcare: the role of artificial intelligence in clinical practice by Shuroug A.Alowais, Sahar S.Alghamdi & others (2023)[9] And 5."The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation" by Bocong Yuan & Jiannan Li (2019)[10] : With the expanding use of big data and artificial intelligence (AI) in healthcare and precision medicine, it appears that robust data protection laws are necessary to guarantee personal privacy. To date, privacy-protecting legislation has been passed countries globally (e.g. in Europe with General Data Protection Regulation — GDP), and health-specific protections are contained within the Health Insurance Portability and Accountability Act (HIPAA) in the U.S.

While the GDPR has established substantial data protection laws inside the EU, causing a dramatic global change in data protection, HIPAA primarily covers pertinent health information supplied by covered businesses.

This study represents an initial effort to evaluate the efficacy of this law reform regarding the protection of personal health data. This study empirically investigates the policy impact of the GDPR on the financial performance of hospitals in the European Union using the difference-

[8] Nitesh naik et al., Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?, (2022), https://www.frontiersin.org/articles/10.3389/fsurg.2022.862322/full..

[9] Shuroug A. Alowais et al., Revolutionizing Healthcare: The Role of Artificial Intelligence in Clinical Practice, (2023), https://bmcmededuc.biomedcentral.com/articles/10.1186/s12909-023-04698-z-

[10] Bocong Yuvan and Jiannan Li, The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation,(2019), https://www.mdpi.com/1660-4601/16/6/1070.

in-difference approach. Findings indicate that hospitals offering digital health services experienced financial difficulties following the 2016 publication of the GDPR. This shows that hospitals all over the European Union made expensive adjustments during the transition period (2016–2018) to comply with the new regulation's requirements for the protection of personal health data. It is possible that the GDPR implementation has seen some initial success.

(B) Research problem

With the increasing concern of patient data theft in India, the need to protect healthcare data is necessary. AI used in healthcare require lots of data as input thus jeopardizing patient privacy and also there is a noticeable gap in studying the deployment of FDA-approved AI programs in other foreign countries that have their own regulatory body for approving AI in Healthcare. The legal and regulatory frameworks addressing issues related to the implementation of artificial intelligence (AI) in healthcare are considerably under-explored. Although AI technologies possess transformative potential in diagnostics, treatment planning, and patient care, the issues of jurisdiction regarding privacy in developing countries remain insufficiently examined in academic literature.

(C) **Research objectives**

This paper aims to compare the regulatory frameworks of AI in countries the US, (a developed nation), India, and Myanmar (developing countries), highlighting the medicolegal challenge (Privacy) posed by AI and its Jurisdiction and exploring the regulatory gaps that persist.

(D) Research question

Whether the existing regulatory framework and legislation available in developing nations effective enough to adapt to the ever-developing medicolegal challenge (Privacy) from the incorporation of AI in healthcare and to decide it’s jurisdiction?

(E) Research methodology

This study adopts a qualitative approach based on a thorough literature review. Some relevant scholarly articles, legal documents, international guidelines, and case studies were reviewed to explore the medicolegal challenges developed by integrating AI into various healthcare systems around the world. The research focused on a comparative analysis of privacy laws and jurisdiction issues related to AI between the United States, India, and Myanmar. The current regulations are analysed on the basis of synthesis from existing literature, and the paper tries to address the gaps left in jurisdiction and privacy in AI-driven healthcare.

II. Privacy framework of the countries

(A) India

A case **Balu Gopalakrishnan v. State of Kerala and Ors**[11] was decided in India in 2020 wherein the confidentiality of patient or COVID-19 individual data is protected by an interim order granted by the Kerala High Court mandating the deployment of protection measures. The Kerala government and the US software company Sprinklr Inc. signed a contract in which the latter agreed to provide an online data platform for the study of health and medical data related to COVID-19. Five petitions were filed in regard to this agreement. In the petitions, it was alleged that there was no protection in the contract against unlawful use of the health information that Sprinklr had gathered on behalf of the State of Kerala. The Court emphasized the necessity, to safeguard the confidentiality of personal data to prevent a "data epidemic." In response to those concerns, the Court mandated the State to anonymize all sensitive personal data collected regarding COVID-19 prior to its transfer to Sprinklr or any third-party service provider. In addition, all future data collection must adhere to the principles of informed consent, i.e., each individual must be informed about the possibility of third parties accessing their data. The Court further ordered Sprinklr to return all remaining COVID-19-related data to the State government and forbade Sprinklr from acting in a manner that would violate data confidentiality.

The importance of individual medical data is regarded highly even when dealing with foreign software. Nowadays the emergence of AI as a transformative force in healthcare is incontrovertible in India.

A study assessing the use of AI in clinical decision-making for 1,000 Indian patients with breast, lung, and colorectal cancers found that between 2016 and 2018, a multidisciplinary tumour board at the Manipal Comprehensive Cancer Centre in Bangalore altered treatment decisions in 13.6% of cases after utilizing Watson's data[12]. The study's importance rests in its illustration of how decision-support tools might influence choices in addition to providing treatment information.

The Department of Health Research, Ministry of Health and Family Welfare, Government of India, along with the Indian Council of Medical Research (ICMR) have partnered with IBM to launch Watson Assistant, a virtual agent, on their portal to address specific questions from

[11] WP (C). No. 22965 of 2020 (S).

[12] Somashekhar, S.P., Sepúlveda, M.J., Shortliffe, E.H., Rauthan, A., Patil, P. and Yethadka, R., 2019. A prospective blinded study of 1000 cases analyzing the role of artificial intelligence: Watson for oncology and change in decision making of a Multidisciplinary Tumour Board (MDT) from a tertiary care cancer center.

front-line staff and data entry operators on COVID-19 from various testing and diagnostic facilities across the nation[13]. In addition to responding about COVID-19 generally, the queries may concern the kind and method of data that test labs must collect, how to keep an inventory of test kits and reagents, the procedure for reporting to different government agencies. Questions were divided into categories such as Staff Training & Testing, Data Entry and Sharing, Governance, and Logistics. As the COVID-19 test network spreads throughout the nation, the virtual agent is also anticipated to assist with the onboarding of new data entry operators and diagnostic center employees.

The Government in order to execute AI initiatives in vital sectors like agriculture and health, NITI Aayog in 2018 has partnered with a number of top AI technology companies. With the motto 'AI for all' (#aiforall), India is setting out to lead the developing world in AI research and application. The Tata Memorial Centre Imaging Biobank is one of NITI Aayog's initiatives[14]. In August 2021, NITI Aayog released the second part of their approach document on Responsible AI.

India's Ministry of Electronics and Information Technology is also one of the government agencies that deals with AI regulations in the country. The Bureau of Indian Standards (BIS), India's national standards body, has created a Divisional Committee on Artificial Intelligence and is currently preparing draft standards for Artificial Intelligence[15].

The attempts of the government of India to regulate AI have been mainly pro-innovation, with it coming out with regulations and guidelines that deal with ethical concerns and risks from AI use which may need the adoption of best practices.

The National Digital Health Mission emphasizes the need to develop laws and guidelines in the health sector to ensure the reliability of artificial intelligence systems.

(B) Legislations ensuring privacy

- **Information Technology Act, 2000**

Existing privacy laws in India are insufficient to control expected levels of data production and dissemination. Section 43A of the Information Technology Act 2000 (the "IT Act") and the Information Technology (Reasonable Security and Procedures and Rules for Sensitive Data or

[13]. ICMR to Leverage IBM Watson Assistant to Bolster Rapid Response to India’s Frontline Testing Facilities on COVID-19,(2020), https://in.newsroom.ibm.com/2020-05-04-ICMR-Watson-Assistant-COVID-19#:~:text=New%20Delhi%2C%20May%204%2C%202020,front%20line%20staff%20and%20data.

[14] national strategy for artificial intelligence #AIFORALL,government of India,(June 2018),https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf.

[15] National Artificial Intelligence Advisory Committee (NAIAC) Share,(2024),https://www.nist.gov/itl/national-artificial-intelligence-advisory-committee-naiac.

Personal Information) Act 2011, made under the Information Technology Act, sets out the data protection framework India has determined that agency companies have "adequate" security controls in place[16]. An organization that does not implement appropriate data protection measures must compensate people affected by the data protection failure. As a data protection "law", this is completely inadequate.

A further issue is that the application of Section 43A is limited to only body corporates, and hence its application is limited to hospitals, and medical facilities which are body corporates, and excludes those that are not. A company is considered a body corporate for the purposes of Section 43A. Clinical institutions are exempt from incorporation under the Clinical Institutions (Registration and Regulation Act, 2010). Hence, even though the majority of hospitals are companies—the All-India Institute of Medical Sciences, for instance, is a body corporate according to Section 3 of the All-India Institute of Medical Sciences, Act, 1956—certain establishments might not be incorporated but the definition of body corporate is “means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities”. This does not exclude the clinical institutions which are not incorporated.

- **Digital Personal Data Protection Act, 2023**

The Digital Personal Data Protection Act, 2023, is a new law passed by India on 11 August 2023. The Act is poised to replace the IT Act, 2000; the Information Technology (Amendment) Act, 2008; and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, once it comes into force. Beyond rights-based protections, the effort intends to create a governing and accountable environment involving data. There will be a significant impact on India's healthcare sector, one still evolving in its digital transformation, imposed by the provisions of the DPDP Act.

The DPDP Act's primary characteristics include[17]

Consent and Data Minimization: Prior to gathering, using, or disclosing a patient's personal information, healthcare professionals must explicitly avail the consent. It ought to be precise, easily retracted, and transparent so that patients maintain ownership over their data. Healthcare institutions are required to guarantee that the information gathered is utilized properly for the

[16] Manisha Singh and Pankaj Musyuni, Digital Health Laws and Regulations India 2024,(2024),https://iclg.com/practice-areas/digital-health-laws-and-regulations/india.

[17] Vijay Pal Dalmia & Rajat Jain, FAQs On The (Indian) Digital Personal Data Protection Act,2020, (October 13 2023), https://www.mondaq.com/india/data-protection/1376950/faqs-on-the-indian-digital-personal-data-protection-act-2023.

intended purpose which will lead to enhancement of data security and patients' trust.

Right to Erasure: The patient is entitled to receive and ask for his or her personal information to be deleted. "Right to be forgotten" is the term for this. Healthcare providers will face logistical difficulties as a result. It should be erased when such withdrawal by the customer is made or if the data are no longer required for the purposes for which they were collected.

This Act obliges the data fiduciaries to notify the Board of Directors of the Data Protection Authority as soon as they become aware of any breach involving personal data. As such this notice must be provided between the time limit set out in the forthcoming regulations and shall never be delayed fly.

Effective policies and processes must be in place for healthcare providers in order to identify, notify, and address breaches involving personal data and to lessen their negative consequences. Serious repercussions may follow for data security and privacy, healthcare organizations' liability and reputation, and even heavy fines may result from this.

III. DATA FIDUCIARY

A "Data Fiduciary" means any individual or business organization determining the purposes and means of the processing of personal data . A Data Fiduciary may themselves process the information or may transfer it to a third party, known as the Data Processor, to process the same in compliance with the provisions of DPDP Act.

A "Significant Data Fiduciary" means any Data Fiduciary or class of Data Fiduciaries notified under this Act by the Central Government.

The DPDP Act has no restriction on cross-border transfer of data. It permits Data Fiduciaries to transfer personal data internationally for processing purposes. Nevertheless, the Central Government retains the authority to impose restrictions on specific countries or regions outside of India regarding such data transfers. Furthermore, the DPDP Act outlines specific responsibilities for Data Fiduciaries, and failure to comply with these obligations may result in penalties reaching up to INR 250 Crores.

The AI mechanisms which collect data for its learning and operation in hospitals and clinics maybe considered as Data fiduciary under this act. This enables the Act to regulate the usage of AI when it does not have a separate legislation

(A) Myanmar

December 2023 – A significant step forward in the improvement and transformation of healthcare in Myanmar has been made with the announcement of a strategic alliance between

EyRIS, the industry leader in AI-driven healthcare solutions, and Advance Innovation[18]. The AI technology, using a basic fundus image as the principal means of increasing screening efforts and bolstering early detection skills for retinal illnesses and chronic disorders.

Chest X-rays are currently reviewed by qXR, an artificial intelligence (AI) technique that is far faster than traditional human review, at Hmwe's clinic and seven other clinics throughout Myanmar. qXR detected 21 new TB cases in 2020[19]. Artificial intelligence (AI) for chest X-rays is proving to be a useful tool in India and Myanmar to address the shortage of radiologists, speed up TB diagnosis, and further the government's goals of eliminating tuberculosis.

15 August 2022 - A Memorandum of Agreement (MOA) was signed by VinBrain and Golden Zanekka Public Company (Myanmar) to implement DrAidTM in top hospitals in Myanmar[20]. According to the MOA, DrAid™ (created by VinBrain) will integrate into the diagnostic process of 3 hospitals in the Golden Zanekka Public (GZK) system - a leading healthcare service provider in Myanmar. In addition to overseeing over ten significant clinics and hospitals in various Myanmar provinces and cities.

(B) Legislations ensuring privacy[21]

- **Constitution of the Republic of the Union of Myanmar (2008)**

Myanmar's 2008 Constitution states in Article 357 that "The Union shall protect every citizen from unlawful intrusion into his privacy and security of home, property, correspondence, and other communications."

This provision plays a much more critical role in the context of the healthcare sector, considering the rapid advancement of AI technologies. Large volumes of personal data, including extremely sensitive health information, are frequently needed for AI systems to operate efficiently. However, the lack of a strong data privacy framework in Myanmar's constitution raises concerns about the level of protection given to people whose healthcare data may be gathered, processed, and examined by AI.

Therefore, Article 357 can be construed as a protective measure against the exploitation of personal information, as healthcare-related data may be regarded as integral to an individual's

[18] Eyris announces partnership with advance innovation in myanmar,(2023),https://www.nova-hub.com/novanews/eyris-announces-transformative-partnership-with-advance-innovation-for-advancing-healthcare-in-myanmar.

[19] Isha Jain,In Myanmar and India, new tech and trusted techniques speed progress against TB,(2021), https://www.path.org/our-impact/articles/myanmar-and-india-new-tech-and-trusted-techniques-speed-progress-against-tb/.

[20] VinBrain cooperates with Golden Zanekka, deploying AI technology in Myanmar,(2022), https://vinbrain.net/vinbrain-hop-tac-cung-golden-zanekka-trien-khai-cong-nghe-ai-tai-myanmar

[21]https://multilaw.com/Multilaw/Multilaw/Data_Protection_Laws_Guide/DataProtection_Guide_Myanmar.aspx

"privacy" and "correspondence[22]." Nevertheless, the section's wording is still insufficient to properly address the intricate moral and legal issues pertaining to data privacy in the AI era. The Constitution may shield citizens from capricious or illegal interference, but it offers no precise rules regarding the gathering, storing, and use of personal health information that is appropriate, especially when it comes to digital or automated systems like artificial intelligence (AI).

- **Electronic Transactions Law (2004)**

This law highlights the trust, integrity, confidentiality, and non-repudiation aspects of data concerning electronic transactions. According to the amended Section 27A of Myanmar's Electronic Transactions Law (ETL), "Person responsible for maintaining personal information" must safeguard it in accordance with its level of sensitivity and refrain from sharing, altering, or disclosing it without authorisation. After data has served its purpose, it must also be deleted. The law encourages data security procedures amongst organisations handling personal data in Myanmar by outlining obligations for data controllers and providing sanctions for non-compliance. Adhering to strict cybersecurity protocols, like encryption and secure authentication, is imperative for healthcare providers and AI developers. The law does not, however, contain any provisions that are specific to artificial intelligence, such as rules governing algorithmic transparency or correcting biases in automation.

(C) The United States

In 2017, US's IBM Watson was under fire for allegedly falling short of expectations about the provision of cutting-edge, individualized treatment for cancer patients, as well as for generating advice that is deemed to be "unsafe and incorrect." It has also tackled concerns like data security, HIPAA compliance, and patient privacy by leveraging its technology and knowledge[23].

(C) Legislations ensuring privacy

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

On August 21, 1996, US legislation (Public Law 104-191) established the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Secretary of HHS (Health and Human Service) is required to publicize the standards it is implementing for electronic

[22] Yuwadee Thean-ngarm and Nwe Oo,Myanmar – Data Protection Overview,(2024), https://www.dataguidance.com/notes/myanmar-data-protection-overview.

[23] Casey Ross, Ike Swetlitz, IBM's Watson supercomputer recommended 'unsafe and incorrect' cancer treatments, internal documents show,(2018), https://www.statnews.com/wp-content/uploads/2018/09/IBMs-Watson-recommended-unsafe-and-incorrect-cancer-treatments-STAT.pdf.

transactions, health information security, and privacy under HIPAA Sections 261 through 264, also referred to as the Administrative Simplification requirements. These rules include financial activities related to health care, such as filing claims or receiving remittances; qualifying and authorizing individuals; and the status of a medical claim. The HHS has set guidelines for transactions involving certain healthcare providers, health plans (as defined by statute), and clearinghouses for health care that electronically transfer any health information are the targets of these regulations. These entities are currently subject to regulations that refer to "covered entities." HIPAA's primary objective was achieved, particularly following HITECH's 2009 amendments[24].

AI technology often relies on extensive datasets for training purposes, which frequently encompass personal information, health-related data, or protected health information (PHI). The incorporation of such data necessitates adherence to data privacy laws and regulations, which will influence the manner in which AI technology utilizes this information.

The HIPAA Privacy Rule imposes considerable limitations on the utilization of Protected Health Information (PHI), mandating that Covered Entities and their Business Associates limit their use of PHI to the minimum necessary to achieve their specific objectives[25]. There are certain exceptions to this rule, such as instances where a Covered Entity discloses a patient's PHI to another Covered Entity for the purpose of treatment, or when a patient is directly informed of their PHI.

According to the HIPAA Security Rule, specifically 45 CFR 164.304, the technical safeguards may address the role of AI in identifying subtle variations and irregularities in data utilization. Additionally, as stipulated in 45 CFR 164.312(d), it is essential to ascertain the manner in which AI is incorporated in discussions concerning the authentication of individuals or entities. Regulations for medical devices, including those powered by AI, are overseen by the FDA.

In January 2024, the Georgia Code was amended by the Georgia Act to amend Article 1 of Chapter 24 of Title 33 of the Official Code of Georgia Annotated (HB887), which forbade the use of artificial intelligence (AI) in healthcare and insurance coverage decisions[26]. Instead, it mandates a meaningful review process and the ability to override any covered decision made with AI.

[24] Jacob Hansen et al., Updating HIPAA Security to Respond to Artificial Intelligence,(2023), https://journal.ahima.org/page/updating-hipaa-security-to-respond-to-artificial-intelligence.

[25] Todd Mayover, When AI Technology and HIPAA Collide,(2024),https://www.hipaajournal.com/when-ai-technology-and-hipaa-collide/.

[26] Airlie Hilliard,The State of Healthcare AI Regulations in the US,(2024), https://www.holisticai.com/blog/healthcare-laws-us#:~:text=Additionally%2C%20section%201851(d).

IV. Jurisdiction

The issue of jurisdictional conflict emerges when multiple states assert their authority over a specific legal matter. This situation frequently occurs in cases that possess an extraterritorial dimension, such as those involving parties from various states or international dealings. Engaging with content or participating in activities online complicates the identification of which national laws, if any, may be infringed. In this regard, nearly every online action carries an international dimension, potentially resulting in overlapping jurisdictions or a spill-over effect.

The worldwide reach of the internet and the unrestricted flow of information have obscured conventional notions of jurisdiction. The challenges posed by AI technologies further intensify these issues, necessitating the development of innovative strategies and frameworks to tackle jurisdictional concerns. Legal cases involving AI frequently span multiple jurisdictions, leading to conflicts that stem from factors such as territoriality, nationality, or the origins and consequences of actions[27].

The application of FDA-approved artificial intelligence in the healthcare sector is prevalent across numerous countries, raising questions of jurisdiction when legal disputes occur. For instance, US's IBM Watson is implemented in India, Thailand, and an additional 24 nations. Furthermore, India has adopted AI technologies from other countries, such as Finland, to improve its medical practices. Such circumstances may create conflicts in the field of jurisdiction. The identification of the appropriate jurisdiction becomes increasingly intricate when artificial intelligence systems possess an international aspect, resulting in difficulties in maintaining legal standards and addressing conflicts.

Promoting arbitration and alternative dispute resolution methods may present flexible and effective solutions for addressing cross-border disputes related to artificial intelligence. Such approaches can facilitate a more versatile resolution process, avoiding the intricacies associated with conventional jurisdictional limitations.

(A) Scope and Limitation

With the evolving nature of AI in this digital era, countries like the US, India, and Myanmar are using their legislature to tackle the problem of protecting the data of individual persons which are used to train the AI which is incorporated in the healthcare sector which has been predominantly used in these countries. The scope is to observe how the pre-existing legislations

[27] https://dig.watch/topics/jurisdiction#ai-and-jurisdiction.

are adjusted to the need when there are no specific AI-regulating laws as India and Myanmar are developing countries. The issue of jurisdiction also arises in situations when AI systems are of the origin of different nations. The limitation of this research is that all the medicolegal challenges are not examined combinedly and the jurisdiction issue is not deeply looked into and has been just mentioned as an emerging crisis.

V. Conclusion

A complex combination of opportunities and medicolegal challenges has emerged with the integration of AI into healthcare systems worldwide. A mosaic of regulatory approaches to AI, data privacy, and jurisdictional matters is revealed by this comparative analysis of the current legislative frameworks in different countries, with each placing a different emphasis on governance. A considerable gap in legal oversight exists because some nations rely on broader, less defined regulations, while others have made progress in developing comprehensive laws tailored to AI, particularly those that address transparency, accountability, and ethical use.

It was found that even in developed country like the US, the existing Act, HIPAA is starting to be criticized with the rise of AI and has led to ideas of Bills such as the Georgia State bill and others that are yet to be passed. India being a developing country has recently passed the DPDP Act, to protect the data of patients but there have been no cases concerning the usage of AI leading to data theft and privacy infringement, the Act's effectiveness is yet to be proved. Myanmar's electronic transaction act, protects the digital data of patients in that country. Although these clauses provide a limited constitutional basis for privacy protection, it falls short of addressing all of the complex issues raised by AI in healthcare.

(A) Suggestion

The liability can be fastened on AI in India and Myanmar if it can be included under the definition of "data fiduciary" and "person responsible for maintaining personal information" respectively for the time being. However, the right to be forgotten cannot be ensured by AI systems as they need data input for further usage. Therefore, the need of new legislation to regulate AI is needed. The issue of privacy is the main concern for this research paper and the other medicolegal challenges are not examined with the legislations available. The country Myanmar was chosen for the reason that it is one of the developing countries that has made a milestone in the AI aspect of healthcare with its first 5D operation in the world with the help of the US. We suggest that the upcoming research could focus on other developing nations' positions in the integration of AI in the field of medicine and their regulating legislation or using other medicolegal challenges. In addition to examining how these countries work with international partners to comply with international standards, this would also include an analysis of how local legal systems are changing to protect patient privacy in the face of AI's rapid development.

*****