INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

ETHICAL AND LEGAL CHALLENGES OF ARTIFICIAL INTELLIGENCE IN MEDICAL FIELD

AUTHORED BY - DHIVYA T[1]

Introduction:

AI applications, along with technologies such as big data and robotics, are expected to have transformational and disruptive potential within the healthcare sector – across various areas such as hospitals and hospital management, pharmaceuticals, mental health and well-being, insurance, and predictive and preventive medicine. However, these applications introduce new risks and challenges that will require policy and institutional frameworks to guide AI design and use. This paper focuses mostly on challenges at the individual level.

With the increasing availability of health-related data, and the use of AI to analyze such data for medical purposes, ethical, technical and resource-related questions will need to be answered. There are quality, safety, governance, privacy, consent and ownership challenges that are still under-addressed. There is also concern among those examining AI design and use that there is a need for humans to understand why and how AI arrived at a specific decision. The processes AI follows, and the speed with which it deals with large amounts of information, are beyond human perception. Many of the algorithms created by ML cannot be easily examined, and it is impossible to understand specifically how and why AI arrived at a specific conclusion. A lack of explain ability and trust in AI processes hampers the ability to fully trust AI systems (Schmelzer, 2019).

In LMICs, some of the challenges of integrating AI into healthcare systems relate to the hurdles of scaling digital health technologies. Other challenges are linked to the fact that LMIC governments lack the resources and technological capabilities to create consistent policies on population health, such as disease burden analysis and monitoring and treatment protocols for use, across their various regions or states. This creates a barrier for AI tools for population health to scale at a national level.' (USAID, 2019) In terms of quality, AI requires high-quality data

[1] The author is working as an Assistant Professor at School of Excellence In Tamilnadu Dr.Ambedkar Law University,Chennai.

ISSN: 2582-6433

in order to produce coherent results. In low-resource settings, this is not always available. A strong digital health infrastructure is required to operate AI tools. Low EMR adoption rates (estimated at less than 40 per cent in LMICs) constitute one of the barriers to feeding AI machines with the necessary historic and real-time patient data (World Bank, 2019; USAID, 2019). Even in high-income countries, the quality of data is a factor determining the speed at which AI tools are put into use. The average UK hospital, for instance, has hundreds of different systems that are not integrated with each other. There is a need for 'an interconnected data infrastructure with fast, reliable and secure interfaces, international standards for data exchange as well as medical terminologies that define unambiguous vocabularies for the communication of medical information' (Lehne et al., 2019).

Protection of citizens' health data is a key area of responsibility for those handling sensitive data for AI purposes. Healthcare organizations will have to respond to growing cybersecurity challenges, and policymakers will have the responsibility of enacting laws that ensure careful governance and security arrangements for stored data. For example, Google DeepMind's partnership with the Royal Free London NHS (National Health Service) Foundation Trust was severely criticized in 2017 for inappropriate sharing of confidential patient data and their use in an app called Streams that was designed to alert, diagnose and detect acute kidney injury. The Royal Free failed to comply with the UK's Data Protection Act when it handed over the personal data of 1.6 million patients to DeepMind. The ruling of the Information Commissioner's Office (the UK's independent authority set up to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals) was based largely on the facts that the app continued to undergo testing after patient data were transferred, and that patients were not adequately informed that their data would be used as part of the test (Information Commissioner's Office, undated; Hern, 2017).

Such instances demonstrate the challenges in developing ethical and legal frameworks for data sharing, interoperability of systems, and the ownership of software produced from such partnerships, as well as the legal framework for clinical responsibility when errors occur (*The Lancet*, 2017).

Privacy concerns are also a critical consideration for the use of data. Health data are most often owned by governments, who could be tempted to sell such data on to private companies. In many cases the users can become the 'product' (in effect, patients' data become monetizable). For

ISSN: 2582-6433

example, in the US, the Walgreens pharmacy chain collects data contained in prescriptions and sends out mailshots about clinical trials related to the customer's illness. For this service, Walgreens is paid a fee by those recruiting patients for clinical trials and by pharmaceutical companies. Kalev Leetaru, writing in *Forbes* magazine, asserts that: '[…] Walgreens does not explicitly inform customers at purchase time that their prescription may be used to target them for medical trials and offer them the ability to opt-out of having their private medical information used in such a manner […]' (Leetaru, 2018). If companies such as Walgreens are able to do this, then it could be the case that technology companies that gather patient information could also sell individuals' sensitive health data to third parties.

There are further ethical considerations. What obligations do technology companies have to alert populations if their AI produces results that reveal society-wide concerns, such as a potential outbreak of a highly contagious infectious disease? Even if technology companies using AI for health purposes report their findings to governments, history has shown that governments can downplay health risks or fail to alert citizens when economic interests are involved. For example, fears over social and economic stability, as well as the political structure involved in alerting of a disease outbreak, led Chinese leaders to delay reporting the outbreak of Severe Acute Respiratory Syndrome (SARS) in 2003 (Huang, 2004).

Governance is challenging in this realm. Health, technology and data protection policies differ greatly across countries and regions, with many LMIC governments lacking the resources and technological capabilities to create consistent policies on population health. At the same time, many of these countries also lack regulations on the use of data and technology that are intrinsic to AI development.

Accuracy must also be considered. A recent report by the UK Information Commissioner's Office highlights the implications around accuracy of personal data during collection, analysis and application. For example, the results of data analysis may not be representative of the wider population, and hidden biases in datasets can lead to inaccurate predictions about individuals (Information Commissioner's Office, 2017). Responsibilities are also not clearly defined. Considering the intricate processes involved in AI-produced results, from data collection to algorithm creation and use, how should a government or regulatory system understand who is responsible for flawed AI-derived recommendations?

ISSN: 2582-6433

Algorithms inevitably reflect the bias of training data, and AI tools tend to show a bias reflecting conditions in the high-income countries where they are developed. This is because the algorithms require millions of historical health datapoints, which are often missing in low-resource settings, to provide accurate outputs appropriate to the geography and population (USAID, 2019). Questions about how the AI's algorithms were designed, and with which inputs, remain to be answered as they are central to the questions of their overall utility and of whether they are appropriate for high-, low- and middle-income settings. A recent study by Facebook's AI Lab demonstrates this hidden bias. Five off-the-shelf object recognition algorithms (Microsoft Azure, Clarifai, Google Cloud Vision, Amazon Rekognition, and IBM Watson) were asked to identify household items collected from a global dataset. '[The] object recognition algorithms made around 10 per cent more errors when asked to identify items from a household with a $50 monthly income compared to those from a household making more than $3,500. The absolute difference in accuracy was even greater: the algorithms were 15 to 20 percent better at identifying items from the US compared to items from Somalia and Burkina Faso.' (Vincent, 2019)

Governments – as well as businesses and non-profit organizations developing AI solutions – also need to consider business model sustainability. This will be a challenge in low-resource contexts, where many of the key actors will not have the financial means to purchase these tools.

Health-related AI applications will require strong infrastructural, legal and ethical frameworks. Government-led initiatives to develop and introduce health-related AI applications, across high-, low- and middle-income settings, need to consider these issues. Governments – as well as businesses and non-profit organizations developing AI solutions – also need to consider business model sustainability. This will be a challenge in low-resource contexts, where many of the key actors will not have the financial means to purchase these tools. As one private insurance company representative in East Africa noted: 'I absolutely see the value of AI risk management tools and I realize that this would save us money, but I do not have the budget to buy something now which will save me money 12 months down the line.' (USAID, 2019) This 'applies to many LMIC governments that understand the value of these AI tools, but do not have the resources to buy them, or the human resources or internal IT capabilities to implement them'. Equity issues do not just apply from country to country, but also arise out of the so-called 'digital divide', where different parts of the same society have differing levels of access to advanced technologies such as 4G networks and smartphones. AI tools for health that are enabled by mobile phone technology are only one example of how more connected populations

ISSN: 2582-6433

and patients will benefit from services such as medical advice and information through devices to which poorer populations may not have access.

Governments engaging with integrating AI tools into healthcare systems will need to take into consideration not just ethical and legal issues (such as privacy, confidentiality, data security, ownership and informed consent) but also fairness, if AI and related technologies are to contribute to achieving the health-related Sustainable Development Goals (SDG) targets. Ubenwa[2] provides existing diagnostics that are 95 per cent cheaper than existing clinical software. The AI used is a ML system that can take an infant's cry as input and analyse the amplitude and frequency patterns in the cry to provide an instant diagnosis of birth asphyxia. The test results from Ubenwa's diagnostic software have shown a sensitivity of more than 86 per cent and specificity of 89 per cent. The algorithm has been used in a mobile app that harnesses the processing capabilities of smartphones to provide near-instantaneous assessment of whether or not a newborn has or is at risk of asphyxia (Louise, 2018). Not only is Ubenwa cheaper, and therefore more easily available in low-resource settings; it is also non-invasive (Ubenwa.ai.). Technology trajectories and their impacts will be shaped by local socio-economic contexts, and thus will not be the same everywhere.

India provides a relevant and useful case study to contextualize some of these issues. The government of India recently released its AI strategy, and healthcare is a priority sector for its application in India (Niti Aayog, 2018a). The government seeks to position India as a 'garage' for developing AI solutions for the rest of the world. Many of challenges facing India – from the type of diseases to the quality of the health infrastructure – are shared by a number of other developing economies.

ETHICAL CHALLENGES:

The use of AI in the clinical practice of healthcare has huge potential to transform it for the better, but it also raises ethical challenges we now address.

1. INFORMED CONSENT TO USE:

Health AI applications, such as imaging, diagnostics, and surgery, will transform the patient–clinician relationship. But how will the use of AI to assist with the care of patient's interface with

[2] An AI application under development in Nigeria, aims to address SDG 3.2 by 2030 (it ends preventable deaths of newborns and children under five years of age)

ISSN: 2582-6433

the principles of informed consent? This is a pressing question that has not received enough attention in the ethical debate, even though informed consent will be one of the most immediate challenges in integrating AI into clinical practice. There is a need to examine under what circumstances, the principles of informed consent should be deployed in the clinical AI space. To what extent do clinicians have a responsibility to educate the patient around the complexities of AI, including the forms of ML used by the system, the kind of data inputs, and the possibility of biases or other shortcomings in the data that is being used. Under what circumstances must a clinician notify the patient that AI is being used at all.

These questions are especially challenging to answer in cases where the AI operates using "black-box" algorithms, which may result from noninterpretable machine-learning techniques that are very difficult for clinicians to understand fully. For instance, Corti's algorithms are "black box" because even Corti's inventor does not know how the software reaches its decisions to alert emergency dispatchers that someone has a cardiac arrest. This lack of knowledge might be worrisome for medical professionals. To what extent, for example,

1. Does a clinician need to disclose that they cannot fully interpret the diagnosis and treatment recommendations by the AI?
2. How much transparency is needed? How does this interface with the so-called "right to explanation" under the EU's GDPR?
3. What about cases where the patient may be reluctant to allow the use of certain categories of data (e.g., genetic data and family history)?
4. How can we properly balance the privacy of patients with the safety and effectiveness of AI?

AI health apps and chatbots are also increasingly being used, ranging from diet guidance to health assessments to the help to improve medication adherence and analysis of data collected by wearable sensors[3] . Such apps raise questions for bioethicists about user agreements and their relationship to informed consent. In contrast to the traditional informed consent process, a user agreement is a contract that an individual agrees to without a face-to-face dialogue. Most people do not take the time to understand user agreements, routinely ignoring them. Moreover, frequent updates of the software make it even more difficult for individuals to follow what terms of service

[3] UK Nuffield Council on Bioethics. Artificial intelligence (AI) in healthcare and research, http://nuffieldbioethics.org/wp-content/uploads/Artificial-Intelligence-AI-in-healthcare-and-research.pdf; 2018 [accessed 01.02.2024].

ISSN: 2582-6433

they have agreed to.

What information should be given to individuals using such apps and chatbots?

Do consumers sufficiently understand that the future use of the AI health app or chatbot may be conditional on accepting changes to the terms of use?

How closely should user agreements resemble informed consent documents?

What would an ethically responsible user agreement look like in this context?

Tackling these questions is tricky, and they become even more difficult to answer when information from patient-facing AI health apps or chatbots is fed back into clinical decision-making.

2. SAFETY AND TRANSPARENCY:

Safety is one of the biggest challenges for AI in healthcare. To use one well-publicized example, IBM Watson for Oncology[4] uses AI algorithms to assess information from patients' medical records and help physicians explore cancer treatment options for their patients. However, it has recently come under criticism by reportedly giving "unsafe and incorrect" recommendations for cancer treatments[5]. The problem seems to be in the training of Watson for Oncology: instead of using real patient data, the software was only trained with a few "synthetic" cancer cases, meaning they were devised by doctors at the Memorial Sloan Kettering (MSK) Cancer Center. MSK has stated that errors only occurred as part of the system testing and thus no incorrect treatment recommendation has been given to a real patient.

This real-life example has put the field in a negative light. It also shows that it is of uttermost importance that AIs are safe and effective. But how do we ensure that AIs keep their promises? To realize the potential of AI, stakeholders, particularly AI developers, need to make sure two key things: (1) the reliability and validity of the datasets and

(2) transparency.

First, the used datasets need to be reliable and valid. The slogan "garbage in, garbage out" applies to AI in this area. The better the training data (labeled data) is, the better the AI will perform. In addition, the algorithms often need further refinement to generate accurate results. Another big issue is data sharing: In cases where the AI needs to be extremely confident (e.g., self-driving

[4] IBM. IBM Watson for oncology, https://www.ibm.com; 2020 [accessed 03.02.24].
[5] 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 05.02.24].

ISSN: 2582-6433

cars), vast amounts of data and thus more data sharing will be necessary. However, there are also cases (e.g., a narrow sentiment AI-based off text) where less data will be required6. In general, it always depends on the particular AI and its tasks how much data will be required.

Second, in the service of safety and patient confidence some amount of transparency must be ensured. While in an ideal world all data and the algorithms would be open for the public to examine, there may be some legitimate issues relating to protecting investment/intellectual property and also not increasing cybersecurity risk. Third party or governmental auditing may represent a possible solution.

Moreover, AI developers should be sufficiently transparent, for example, about the kind of data used and any shortcomings of the software (e.g., data bias). We should learn our lessons from examples such as Watson for Oncology, where IBM kept Watson's unsafe and incorrect treatment recommendations secret for over a year. Finally, transparency creates trust among stakeholders, particularly clinicians and patients, which is the key to a successful implementation of AI in clinical practice.

The recommendations of more "black-box" systems raise particular concerns. It will be a challenge to determine how transparency can be achieved in this context. Even if one could streamline the model into a simpler mathematical relationship linking symptoms and diagnosis, that process might still have sophisticated transformations beyond the skills of clinicians (and especially patients) to understand. However, perhaps there is no need to open the "black box": It may be that at least in some cases positive results from randomized trials or other forms of testing will serve as a sufficient demonstration of the safety and effectiveness of AIs.

3. ALGORITHMIC FAIRNESS AND BIASES:

AI has the capability to improve healthcare not only in high-income settings, but to democratize expertise, "globalize" healthcare, and bring it to even remote areas. However, any ML system or human-trained algorithm will only be as trustworthy, effective, and fair as the data that it is trained with. AI also bears a risk for biases and thus discrimination. It is therefore vital that AI makers are aware of this risk and minimize potential biases at every stage in the process of product development. In particular, they should consider the risk for biases when deciding (1) which ML

[6] Figure Eight. What is training data?, https://www.figure-eight.com/resources/what-is-training-data; 2020 [accessed 05.02.2024].

ISSN: 2582-6433

technologies/procedures they want to use to train the algorithms and (2) what datasets (including considering their quality and diversity) they want to use for the programming.

Several real-world examples have demonstrated that algorithms can exhibit biases that can result in injustice with regard to ethnic origins and skin color or gender[7]. Biases can also occur regarding other features such as age or disabilities. The explanations for such biases differ and may be multifaceted. They can, for example, result from the datasets themselves (which are not representative), from how data scientists and ML systems choose and analyze the data, from the context in which the AI is used, etc. In the health sector, where phenotype- and sometimes genotype-related information are involved, biased AI could, for instance, lead to false diagnoses and render treatments ineffective for some subpopulations and thus jeopardize their safety. For example, imagine an AI-based clinical decision support (CDS) software that helps clinicians to find the best treatment for patients with skin cancer. However, the algorithm was predominantly trained on Caucasian patients. Thus, the AI software will likely give less accurate or even inaccurate recommendations for subpopulations for which the training data was under inclusive such as African American.

Some of these biases may be resolved due to increased data availability and attempts to better collect data from minority populations and better specify for which populations the algorithm is or is not appropriately used. However, a remaining problem is that a variety of algorithms are sophisticated and nontransparent. In addition, as we have seen in the policing context, some companies developing software will resist disclosure and claim trade secrecy in their work. It may therefore likely be left to nongovernmental organizations to collect the data and show the biases.

In cases of "black-box" algorithms, many scholars have argued that explain ability is necessary when an AI makes health recommendations, especially also to detect biases. However, does this view really hold true? Some argue that what matters is not how the AI reaches its decision but that it is accurate, at least in terms of diagnosis. The safety and effectiveness of health AI applications that are "black boxes" could, for example, be demonstrated—similar to the handling of drugs—by positive results of randomized clinical trials.

[7] Short E. It turns out Amazon's AI hiring tool discriminated against women. Silicon Repub, https://www.siliconrepublic.com/careers/amazon-ai-hiring-tool-women-discrimination; [accessed 05.02.2024].

ISSN: 2582-6433

A related problem has to do with where AI will be deployed. AI developed for top-notch experts in resource-rich settings will not necessarily recommend treatments that are accurate, safe, and fair in low-resource settings. One solution would be not to deploy the technology in such settings. But such a "solution" only exacerbates preexisting inequalities. More thought must be given to regulatory obligations and resource support to make sure that this technology does improve not only the lives of the people living in high-income countries but also of those people living in low- and middle-income countries.

4. DATA PRIVACY:

In July 2017, the UK Information Commissioner's Office (ICO) ruled that the Royal Free NHS Foundation Trust was in breach of the UK Data Protection Act 1998 when it provided personal data of circa 1.6 million patients to Google DeepMind[8]. The data sharing happened for the clinical safety testing of "Streams," an app that aims to help with the diagnosis and detection for acute kidney injury. However, patients were not properly informed about the processing of their data as part of the test. Information Commissioner's Elizabeth Denham correctly pointed out that "the price of innovation does not need to be the erosion of fundamental privacy rights".

Although the Streams app does not use AI, this real-life example has highlighted the potential for harm to privacy rights when developing technological solutions. If patients and clinicians do not trust AIs, their successful integration into clinical practice will ultimately fail. It is fundamentally important to adequately inform patients about the processing of their data and foster an open dialog to promote trust.

The lawsuit Dinerstein v. Google and *Project Nightingale* by Google and Ascension are recent case studies showing patient privacy concerns in the context of data sharing and the use of AI.

But what about the ownership of the data? The value of health data can reach up to billions of dollars, and some evidence suggests that the public is uncomfortable with companies or the government selling patient data for profit. But there may be ways for patients to feel valued that do not involve ownership per se. For example, the Royal Free NHS Foundation Trust had made a deal with Google DeepMind to provide patient data for the testing of Streams in exchange for

[8] ICO. Royal Free—Google DeepMind trial failed to comply with data protection law, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law; 2017 [accessed 06.02.2024].

ISSN: 2582-6433

the Trust's free use of the app for 5 years. Reciprocity does not necessarily require ownership, but those seeking to use patient data must show that they are adding value to the health of the very same patients whose data is being used.

Beyond the question of what is collected, it is imperative to protect patients against uses outside the doctor–patient relationship that might deleteriously affect patients, such as impacts on health or other insurance premiums, job opportunities, or even personal relationships. Some of this will require strong antidiscrimination law—similar to regimes in place for genetic privacy; but some AI health apps also raise new issues, such as those that share patient data not only with the doctor but also with family members and friends. In contrast to the doctor who is subject to duties of confidentiality set out by governing statutes or case law, family members or friends will probably not have legally enforceable obligations of such kind.

LEGAL CHALLENGES:

While artificial intelligence ("AI") is used across sectors, the application of AI in the healthcare sector assumes substantial significance. Law will need to catch up and keep pace with new innovation in order to ensure full potential is exploited from such innovation.

There are several ways in which AI is being used or proposed to be used in the healthcare industry which mainly include data collection, data storage, data analysis, monitoring conditions, prescribing treatments, AI assisted robotic surgeries. Hospitals, pharmaceutical companies, diagnostic companies, fitness wearables and telemedicine are some of the businesses in the healthcare sector which use AI.

However, the regulatory framework in India has not been updated to keep abreast with developments.

1. LIABILITY ISSUES:

At present, a medical professional is responsible in case a deficiency of his/her duty leads to negligence. There have been instances of civil as well as criminal penalties being imposed on medical professionals in the past for negligence. The regulations do not, however, distinguish cases where there is an error in diagnosis malfunction of a technology, or the use of inaccurate or inappropriate data. As a result, presently there is no accountability for the software developer

ISSN: 2582-6433

developing the AI solution or the specific program engineer who designed it. It is also unclear on how one determines the level of accountability of the medical professional when he/she provides the wrong treatment or diagnosis due to a glitch in the system or an error in data entry.

For instance, publicly available data suggests that certain AI solutions created for treating cancer patients have had instances of giving unsafe recommendations. Reports have suggested that cancer patients with severe bleeding have been recommended a drug that could cause the bleeding to worsen. Under the current regulations in India, the medical professional can be held accountable for prescribing the relevant drug and may not be able to take a defence that he/she relied on the recommendation of an AI solution.

2. DATA PRIVACY:

The use of AI would entail a constant exchange of information between the patients and the AI service provider. These create massive datasets which are then processed for training, validation and creating algorithms. The lack of adequate data privacy laws in India could result in such data sets being commercially exploited for matters beyond development of AI solutions.

Recognizing the issue, earlier this year, the Ministry of Health and Family Welfare released a draft of the Healthcare Security Act. In addition to the electronic health record standards, this law proposes to provide civil and criminal remedies for breach of data and principles for data collection and use. It also provides for the establishment of the National Digital Health Authority, a regulator which will focus exclusively on enforcing healthcare data protection norms.

3. IPR REGIME:

The intellectual property regime in India does not recognize patentability of algorithms, the basis on which an AI solution functions. In fact, the Patents Act expressly exempts algorithms from being “inventions” eligible for patent protection. This regime may result in being averse to incentivizing development of AI solutions.

Also, AI algorithms are created by collating and analyzing human-created works and data-sets. Indian laws grant copyrights to creators of the work with the exclusive right to reproduce their works. It is unclear whether creating copies of these works and datasets (without the consent of the creator) for developing AI solutions could be viewed as copyright infringement by the developer.

ISSN: 2582-6433

Presently, AI in healthcare does face regulatory challenges (some of which have been highlighted above) which can be resolved only by formulating an effective regulatory framework to ensure sufficient oversight on AI. While the technology is fast changing, and AI will play an increasingly important role in healthcare in India, the India laws will also need to be developed and amended constantly to adequately regulate the role of AI in the healthcare sector. India could consider forming a committee entrusted with the task of evaluating the operation of AI-driven solutions and suggesting changes to Indian regulations.

Further, under the IPR regime, the Patents Act expressly exempts the patentability of algorithms from being 'inventions' eligible for patent protection. However, since the algorithms are created by collating and analyzing human created work, the creator of the work can be granted copyright under the Indian laws with the exclusive rights to reproduce their own work. While addressing the question of accountability, AI system has been envisaged as only a decision-support system and is thus not intended to replace the doctors. It will help in providing first layer screening interpreted by the human and he will be responsible to point out errors if any.

4. DATA ACCESS:

These AI systems are always dependent on the availability of large data access of their consumers, working the healthcare system on AI requires a lot of access of the patient's previous medical history, records etc., which would be quite a challenge in India, especially in rural and semi-rural areas, where these records and data aren't managed well.

5. BLIND SPOTS IN DATA COLLECTION:

Currently, there are a lot of caste, gender, and class based irregularities in the medical systems in many areas of the nation, many lower cast women are denied of proper health care because of certain practice of elitism in those areas, this leads to fewer representation of a certain type of data in the medicine formulation, which in turn may be effective for only a certain amount of people in the population, and not all of them.

6. HIGHER COSTS:

The whole structure employed in the AI systems is very expensive; the costs of training, testing, and deploying AI systems are very high. Collection of data is also expensive in itself, and most of the Healthcare companies would be relying over cloud services of foreign companies, because they don't have that much of Technological support.

ISSN: 2582-6433

7. ACCOUNTABILITY:

A computer most certainly cannot be held accountable in case of occurring of any error or misdiagnosis. There has to be a human in the loop, They AI systems should not be intended to replace doctors. Current Legal Framework and Implications Currently, the medical professional is held responsible for any deficiency or negligence in his/her services. Due to absence of any specific law enacted to deal with AI and the advanced technology in India it is difficult to distinguish cases where the error occurs in diagnosis malfunction of technology or use of inaccurate data. The healthcare organizations will have to face the growing cybersecurity challenges besides the policymakers will have the responsibility of enacting laws ensuring careful governance and security arrangements for stored data. Currently, the cases relating to AI in healthcare might be governed under other laws or acts like the COPRA (Consumer Protection Act), as the patient is a consumer using the services provided by the AI systems, and in case of any default may take any course of action according to COPRA, for instance, if a patient has been prescribed a certain drug, which contributes towards worsening his condition, he will have a remedy under the COPRA.

Similarly, if any patient's personal information is being shared or either being leaked by mistake or any error in the AI system, and which the concerned company isn't authorized to do so, may face certain legal implications under the Data Protection and Privacy laws of India. Admittedly, there is a void in the legal and regulatory framework affecting Artificial Intelligence. On one hand the AI applications along with supporting technologies are expected to bring transformative changes on the other hand it has disruptive potential in the healthcare sector across hospitals and hospital management, mental health and well-being, pharmaceuticals, insurance and medicine. The adoption of AI in healthcare sectors would require policy and institutional framework to guide and design the use of Artificial Intelligence system. With the availability of health related data, another challenge would be to address the questions of ethical, technical and legal nature.
The questions as to quality, safety, governance, privacy, consent and ownership poses a greater challenge that is still under-addressed. Another concern regarding the use and designing of AI is that it would be examining why and how AI has reached to a specific decision. Right to Privacy being fundamental right demands for citizen's health data to be protected and therefore it becomes the key responsibility of those handling the sensitive data for AI purposes.

The use of AI based solutions entails constant exchange of information between the patients and AI service provider. Such exchange creates massive datasets which are further processed for

ISSN: 2582-6433

training, validation and creating algorithms.

Therefore, the lack of adequate data privacy laws in India results in commercial exploitation of the datasets leading to challenges termed as 'Black Box Phenomena' that is beyond development of AI solutions Owing to the violation of privacy the Ministry of Health and Family Welfare released a draft of the Healthcare Security Act. The Act proposes to provide civil and criminal remedies for any breach of data and principles of data collections and its use. The Act also provides for institution of the National Digital Health Authority as a regulatory authority which will focus exclusively on enforcing healthcare data protection norms.

CONCLUSION:

AI will support the future needs of medicine by analyzing the vast amounts and various forms of data that patients and healthcare institutions record in every moment. AI is likely to support and augment physicians by taking away the routine parts of a physician's work hopefully enabling the physician to spend more precious time with their patients, improving the human touch. While AI is unlikely to replace physicians in the foreseeable future, it is incumbent on medical professionals to learn both the fundamentals of AI technology as well as how AI-based solutions can help them at work in providing better outcomes to their patients. Or, it might come to pass that physicians who use AI might replace physicians who are unable to do so.

As the number of AI applications grows and the technology develops, applying it without due care could lead to problematic outcomes, as well as public reluctance to accept or use it. As devices get smarter, they rely more on algorithms to make suggestions (e.g. showing the links between behavior, biometrics and disease) and take actions (e.g. surgery-assisting robots). This could result in ineffective actions if the data that decisions are based on is: incomplete and thus unreliable, vulnerable to tampering by cyber-attackers, possibly biased, or simply incorrect. This requires a fresh look at how we make sure these approaches will have the intended effects. It therefore becomes essential that such algorithms are subjected to transparent standards in approval procedures. These barriers can be overcome with the collaboration of all stakeholders in the ecosystem: policy makers at all levels, healthcare providers, academia, industry and citizens. With this broad partnership, AI innovation and adoption can help ensure high-quality care for citizens and put the country at the forefront of a very innovative industry.