Right to Privacy and Confidentiality of Patient Data in the age of AI: Legal obligations of Medical Professionals to Protect Patient Information

Jyotsana Singh[1], Aparajita Singh[2]

[1]5th Year, BA LLB, Student, Symbiosis Law School, Hyderabad
[2]2nd Year, BBA LLB, Student, Symbiosis Law School, Pune

Abstract

The advancements in adoption of Artificial Intelligence (AI) technology in the healthcare industry have been very execute rapid and have brought very efficient change in the functionality, diagnostics, and management of the healthcare industry. But this technological advancement come with very significant question and issues on the right to privacy and confidentiality of patient data especially in India following the constitutional provision that privacy is a right under the Article 21 of the Constitution. The gap in the research specifically relates to whether the contemporary legal instruments that include the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, the Information Technology Act, 2000 and the proposed Digital Personal Data Protection Act, 2023 adequately respond to the challenges raised by the AI healthcare technologies emerging in the healthcare sector. One major research issue derives from the enormous data-handling capability of the AI systems with possible infringement of identity rights, apply bias and abusive of 'patients' sensitive health information. As mentioned earlier, this research investigates how effectively Indian law protects privacy and confidentiality in AI health systems. It also assesses the legal and ethically responsible implications of doctors and other healthcare workers in terms of Patient's data privacy in their usage of the AI tools. The other important dimension of this research is to identify how the Indian law and policy may be reframed to reduce the privacy vulnerability. Using the AI in the process, new problems arose: the definition of informed consent within the agreements of data sharing and AI's responsibility regarding the automated decision-making process. This study also discusses what could be learned from other nations by developing an effective regime for the regulation of AI in healthcare in India with reference to GDPR and HIPAA. In addressing these dimensions, the study seeks to fill the identified gap in the existing literature by offering insights regarding the roles and responsibilities of physicians and health policy makers in realising the potential of AI while ensuring patient confidentiality at the same time. The insights generated out of the study will help in formulating the legal guidelines that can encompass accountability, ethical standards and public confidence in technologies embedded in the health care systems.

Keywords: Artificial Intelligence, HealthCare, Right to Privacy, Data Protection, Ethics, Patient Privacy

Introduction

Academic breakthrough in Artificial Intelligence in healthcare is ushering in an era of medical innovation where diseases are diagnosed, treated and managed differently. Machine learning algorithms and predictive analytics with the help of AI, have enabled clinical decision making to go to a maximum level of accuracy by finding patterns of data in huge data sets. Not only are such technologies as AI driven imaging systems, robotic surgeries, personalized medicine helping improve patient outcome, they are also helping ease the delivery of healthcare. Specifically, as an example, AI apps in radiology have put an end to conditions such as cancer, and AI algorithms in pharmacology have speeded up development of drugs. With growing digitization of medical records and adoption of electronic health records (EHRs), AI can seamlessly expand the ways into the world of healthcare leading to that rapid integration. But now Health care providers can analyse the mountains of patient data to give them more efficient and personalized treatment. On the one hand, the intense reliance on data driven technologies has thrown up enormous questions as to how to handle, secure and exchange sensitive patient information, and this needs to be resolved through a strong legal framework.

In the healthcare industry, patient data can often be pretty sensitive, it’s medical history, genetic information, even things like personal identifiers. Guarding this information is not just a legal thing to do, but also an ethical thing to do: This is behind the trust between patients and healthcare providers. Very bad consequences they can lead to identity theft, discrimination or use of health information for commercial purposes are among a number of confidentiality breaches.

It recognizes people's autonomous and dignity and hence believes in protecting the right of the privacy as a fundamental right under Article 21 of the Indian Constitution. With large datasets processed and shared continuously in the context of AI, particularly confidentiality and privacy issues become more complicated. While efficient, AI systems operate as black boxes and while we may know they sometime get it right and sometimes get it wrong, we don’t always know how they got it right or wrong. Such lack of transparency raises questions about the level of informed consent, and accountability, and of course biases inherent in these systems.

Then, AI exposes the risk of breaches by being able to aggregate data from several sources at once. The current data protection infrastructure has also been provided further reason to be eroded by cyberattacks on healthcare organizations. As the application of AI technologies to health care steadily increases, these privacy concerns need to be addressed to create ethical practices and maintain public trust with AI in health care.

This is a study that fills a huge gap in the literature in terms of understanding how Indian laws are pertaining to the incredibly fast pace of technological advancement in the AI based healthcare. The learning is also centered around international benchmarks, such as the GDPR and HIPAA, to find out which practices would be best to adapt in order to make policy for India.

This research seeks to understand how AI tools can help enrich and enhance the healthcare delivery process while observing legal and ethical dimensions to help healthcare providers bear their responsibilities towards protection of patient data. Its purpose is to contribute to this formulation of an appropriate balance between innovation and accountability for AI technologies with no impact on the exercise of healthcare rights.

The focus of this study is to analyze the level of the adequacy of Indian legal frameworks to safeguard patient data privacy in an era of AI. Additionally, it also tries to examine the ethical and legal duties of medical doctors regarding this case and recommend actionable suggestions to enhance regulatory devices.

Legal Framework Governing Patient Data Protection in India

Privacy is of a fundamental right as per Article 21 of the Indian Constitution,[1] guaranteeing the right to life and personal liberty in the Supreme Court ruling KS Puttaswamy v. UOI 2017[2] the recognise privacy as a cornerstone of human dignity, personal decision making, and informational self-determination. The Indian medical Council regulations, 2002, emphasise patient confidentiality, but lack provisions for rapid technology advancements like AI that is artificial intelligence and the new advancements further more the IT act 2000, provide safe cards but remains outdated in addressing the complexities of AI driven healthcare and different telemedicines platform[3] The newly passed 2023 DPDP act is a forward-looking approach in the new era of artificial intelligence. This law requires the owner's mutual consent for processing sensitive data, empowers individuals to correct or delete their information. As technology continues to redefine healthcare delivery, India legal landscape must strike a balance between innovation and privacy to promise dignity and liberty Examination of constitutional provisions (Article 21 and the Right to Privacy judgment).

The right to privacy, a fundamental tenet of indivitual autonomy right to privacy is recognized as an inherent right under Article 21 of the Constitution of India as the right to life and personal liberty. The historic judgment **K.S. Puttaswamy (Retd.) v. Union of India (2017)[4]** specifically laid down a very categorical view that privacy amounted to an essential facet of human dignity and freedom, marking a turn in Indian constitutional jurisprudence.

It made privacy an integral attribute of human dignity and freedom as an identity mark in Indian constitutional jurisprudence. Freedom in economy and existentialism is thus an interactive dimension of the psyche. They all belong to a larger whole comprised of the human elements that deserve recognition as essential under the right to life and personal liberty enshrined in Article 21[5]. Even if the provision does not explicitly mention privacy, it is interpreted by the Supreme Court to extend the scope of the provision. Once, Article 21[6] was associated explicitly with procedural safeguards against arbitrary action by the state until a few years back. By then, these judicial pronouncements had shifted to substantive rights and included shelter, education, and health as determined and protected by law within the framework of Article 21[7] itself. The concept of privacy as a constitutional right can be traced to **Kharak Singh v. State of Uttar Pradesh (1964)**[8], where the Supreme Court held that unauthorised surveillance violates personal liberty. Insofar as it has not held that privacy should be regarded as a right unto itself since the view held by the majority is based on physical intrusion.

Subsequent cases like Gobind v. State of Madhya Pradesh (1975)[9] have considered privacy as part of personal liberty but subject to reasonable restrictions. Justice KS Puttaswamy v Union of India: The Dark

[1] Privacy in the Age of Artificial Intelligence: An Indian Perspective, 17.2 UILS (2023) 114
[2] K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (India)
[3] Healthcare Challenges : Artificial Intelligence Promises Quantum Leap, 6.1 RSRR (2020) 182
[4] ibid
[5] Constitution of India, art 21
[6] ibid
[7] ibid
[8] Kharak Singh v State of Uttar Pradesh (1964) 1 SCR 332 (India)
[9] Gobind v State of Madhya Pradesh (1975) 2 SCC 148 (India)

Horse Regarding the Aadhaar scheme, the petitioner contended that the collection by the government of biometric data while providing public services was infringing privacy without safeguards[10]. This was a unanimous hold by a nine-judge bench of the Supreme Court that such privacy is inherent under Article 21[11].

It elaborated on the philosophical, legal, and constitutional dimensions of privacy and stated that privacy protects individual autonomy, freedom of decision-making, and human dignity.privacy-related rights include rights pertaining to bodily integrity, informational self-determination, and personal relationships, which form the core of human rights.[12] The judgment also pointed out that the imposition of privacy gives other basic rights a sense of meaning, for example, the right under Article 19(1)(a)[13] to freedom of speech, which involves the freedom to speak privately. In addition, it will add to the constitutional mandate on the legality of the Information Technology Act, of 2000 and the proposed Digital Personal Data Protection Act of 2023.

The development of privacy as a Fundamental right under Article 21[14] brings overwhelming implications for human dignity and freedom. The Puttaswamy judgment has not only broadened the significance of Article 21[15] but also laid a solid groundwork to safeguard individual rights in this digital age, including in sensitive fields such as health care.

Analysis of existing regulations:

1. Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.

These regulations made in 2002 under the Indian Medical Council IBH Act, 1956, are basically meant to be the indisputable code of conduct for all medical practitioners in India.[16] These regulations advocate the dignity of the medical profession as well as the welfare of patients, while also establishing confidence in healthcare providers and the public. It also opens the way for the confidentiality of patients, which is a critical issue.[17] The 2002 Regulation provides an exhaustive code of conduct to registered medical practitioners (RMPs) in India. It has many areas, encompassing ethical principles for patient confidentiality, informed consent, professional competence, and prohibition against malpractice. Their ethical duties as medical practitioners toward their patients, fellow colleagues, and society as a whole have been emphasised within clauses 1.1-8.6 of the regulations[18].

Among these provisions, Clause 7.14[19] stipulates explicitly that the patient information must 100 percent be kept confidential. RMPs are ethically bound by Clause 7.14[20], which requires that no patient secret learned through professional practice should be divulged by RMPs except on the authority of law or at the patient's consent. This is a very essential confidentiality that allows the development of trust between the

[10] K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (India).

[11] Constitution of India, art 21

[12] Privacy in the Age of Artificial Intelligence: An Indian Perspective, 17.2 UILS (2023) 114

[13] Constitution of India, art 19(1)(a)

[14] Constitution of India, art 21

[15] ibid

[16] Digital Health in India - Key Trends and Impact of Regulation, 6.1 RSRR (2020) 1

[17] ibid

[18] Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002, cls 1.1–8.6.

[19] Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002, cl 7.14

[20] ibid

doctor-and-patient relationship, and facilitates good diagnosis and treatment.[21] All these Electronic Health Records (EHRs), telemedicine platforms, and feasibility made available through artificial intelligence (AI) could require data sharing among stakeholders to create suspicion based on unauthorized access and misuse.

The 2002 Regulations talk about confidentiality in principle but do not deal with how to handle clinical health data, especially with regard to the current issue of AI in Healthcare. For one, diagnostic tools deploying artificial intelligence require massive patient data for training the algorithms, creating loopholes for unauthorized users to access the data and misuse it.[22]

These 2002 Regulations also have relations with other legal instruments, such as the Information Technology Act, of 2000 and the recently proposed Digital Personal Data Protection Act of 2023. Further, the 2023 Act provides principles of purpose limitation and accountability not less than the norms of ethics for patient confidentiality. The collision of frameworks entails their compatibility. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, is still an important unit for ethical medical practice in India. Digitalisation in healthcare requires a more dynamic and adaptive regulatory approach. This can strengthen the 2002 regulations to deal with evolving technologies, and merging them with statutory data protection laws.

2. Information Technology Act, 2000.

The establishment of the landmark legislation referred to as the Information Technology Act in India in 2000. The IT Act offers a mandate for the recognition of electronic records and digital signatures; it also provides legal mechanisms against cybercrime and makes provisions to protect sensitive personal data, including health-related information.[23] It also protects the patient's curated and private data, which includes e-health records, telemedicine, and AI in diagnosis, among others. The IT Act mainly protects patients from their data being accessed in the healthcare sector. Although the Act was primarily intended to provide a legal framework for the regulation of cybercrimes and ease to facilitating electronic commerce range, it has very considerable consequences to privacy concerning personal data, especially in sectors such as health, where personal data is being digitally processed.[24]

The most important thing to highlight from the IT Act is the regulation concerning sensitive personal data in Section 43A,[25] Which mandates that corporate bodies institute reasonable security practices in the safeguarding of sensitive personal data from unauthorised access, disclosure, and misuse. Key Provisions and Effect on Healthcare The IT Act has some of the provisions that are very relevant in connection to patient data protection within digital healthcare. Section 72A[26] of the IT Act makes it a criminal act to disclose personal information acquired during the course of rendering such services, which include health-related information.[27] The protection of patients' privacy is defined herein through the punishment of individuals who unethically exploit their privilege for accessing personal data specifically in such cases when the information is shared without consent.

[21] Digital Health in India - Key Trends and Impact of Regulation, 6.1 RSRR (2020) 1

[22] Alhammad N, Alajlani M, Abd-alrazaq A, Epiphaniou G, Arvanitis T Patients 'Perspectives on the Data Confidentiality, Privacy, and Security of mHealth Apps: Systematic Review J Med Internet Res 2024;26:e50715

[23] Digital Health in India - Key Trends and Impact of Regulation, 6.1 RSRR (2020) 1

[24] ibid

[25] Information Technology (Amendment) Act, 2008 (No. 10 of 2009), Section 43A, The Gazette of India, Feb. 5, 2009

[26] Information Technology (Amendment) Act, 2008 (No. 10 of 2009), Section 72A, The Gazette of India, Feb. 5, 2009

[27] Data privacy in india: The information technlogy act by benjamin wilson

Further, as per Section 43A[28] of the Act, any organization which processes sensitive data should ensure that it adopts "reasonable security practices and procedures." This, indeed, has far-reaching consequences for healthcare providers who must take care of the electronic storage of patient information.[29] Medical institutions and professionals collecting and storing profession-related patient health data electronically must comply with industrial data security standards in terms of keeping the data secure and encrypted, with a view to preventing data breaches.

While the IT Act does provide a legal umbrella for data protection in digital spaces, the parts of this act concerning data protection do not set out the particularities of guidelines and standards for healthcare data protection and, above all, in the developed challenges caused by new technologies like A.I., which will gather huge amounts of sensitive data belonging to patients. However, there is an urgent need to align its provisions with emerging privacy frameworks such as the Digital Personal Data Protection Act, 2023 and the General Data Protection Regulation (GDPR) of the European Union. The 2023 Data Protection Act, which establishes the comprehensive legal framework for personal data protection, basically adds to the IT Act through its specific provisions relating to the processing of sensitive personal data, including health data.

3. Digital Personal Data Protection Act, 2023[30]

The Digital Personal Data Protection Act 2023[31] is a key bill in New Indian Legislation which has been a growing legal area there covering effective data protection laws. It speaks to a greater importance of data protection, considering that the country has seen radical digital transformations, as it has become apparent that many industrial sectors, particularly health, are clamouring for a law adjuration of data issues. However, the buffer draft DPDPA was made chiefly to address rules and regulations regarding the effective collection, storage, processing, and sharing of personally identifiable information to assure individuals' privacy rights. Also, the adoption of this Act will probably have serious effects on health care and other sectors related to sensitive personal data such as information about health.

The primary goal of the DPDPA is to establish a strong mechanism for protecting personal data while promoting the growth of digitalisation in the economy. The Act extends to the processing of personal data within India and, in certain cases, to processing outside of India, provided the data pertains to individuals within the jurisdiction of India.[32]Thus, it imposes certain purposes for which the data should be collected and provides that retention is not for longer than necessary.

Sensitive detail such as that associated with health data in DPDPA is also very critical in its consideration. Explicit consent from the individual is required before the organization processes sensitive personal data, as the Act states. This is perhaps one of the biggest steps towards patient privacy since patients have more control over who accesses and uses their health data.

The Act specifies that data processors, such as hospital institutions, health workers, or AI-run platforms in the field of healthcare, should adopt strict security to ensure the safety of personal data it is holding. One of these is data encryption, access control, and frequent check-ups to ensure compliance with the provision of the Act. The provisions seem crucial for the health industry because of the high sensitivity of their activities in handling the personal data amounting to huge volumes and susceptible to having a risk

[28] Information Technology (Amendment) Act, 2008 (No. 10 of 2009), Section 43A, The Gazette of India, Feb. 5, 2009

[29] Data privacy in india: The information technlogy act by benjamin wilson

[30] The Digital Personal Data Protection Act 2023, Act No 22 of 2023 (India)

[31] Privacy in the Age of Artificial Intelligence: An Indian Perspective, 17.2 UILS (2023) 114

[32] ibid

of considerable ease of exploitation when not well protected. The DPDPA therefore strengthens the rights individuals can exercise regarding their personal data: right to access, correction, erasure, and data portability. Thus, in regard to the healthcare sector, it implies that a patient can demand access to their health records while requesting correction in case a mistake exists in the record. In addition, a patient may request deletion of the health data if no longer necessary or if consent is otherwise withdrawn. It emphasizes that healthcare providers, including hospitals and telemedicine platforms, must obtain informed consent from patients before collecting[33]

The Act further provides for Data Fiduciaries-that is, the organizations that are charged with the management of personal data. Healthcare providers fall into this category under the DPDPA whereby they are legally bound to the principles of the DPDPA in processing patient data in an ethical and transparent way.[34] The Primary Step in data protection is crucial, yet the Indian Government may face challenges in implementing the Data Protection Bill. Concerns about potential misconduct are rising, especially in the medical field, where the use of personal data with new technologies like IT and machine learning is more common compartively to last decade.

Thus, The Digital Personal Data Protection Act 2023 it aims to significantly enhance personal data protection in India, especially to sensitive health related information. As technology advances, digital enterprises in healthcare must evolve to ensure safeguards for the future.[35]

AI in Healthcare: Opportunities and Challenges

"I think AI is coming about and replacing routine jobs is pushing us to do what we should be doing anyway: the creation of more humanistic service jobs."[36] - Dr Kai-Fu Lee, Chairman and CEO of Sinovation Ventures[37]

The WHO defines digital health as "a broad umbrella term encompassing eHealth as well as emerging areas, such as the use of advanced computing sciences in big data and artificial intelligence[38]

In recent years, AI has seen a revolutionary change in the healthcare sector due to the growing adoption of artificial intelligence in different sectors. The field of medical diagnosis, therapy and patient care is in a transformative phase after the recent increase of AI in the medical field. Artificial intelligence can now analyse complicated medical pictures, MRI and CT scans along with X-rays more accurately and efficiently than humans can. A recent study by Nature Medicine stated that AI surpassed humans by detecting evolving breast cancer cells in mammograms [39] However, How successfully artificial intelligence is integrated into healthcare will ultimately depend on how well it can preserve patient privacy while leveraging the benefits of the technology. The healthcare sector may use AI to improve patient outcomes while respecting individual rights if privacy and ethical issues are approached proactively.

[33] Privacy in the Age of Artificial Intelligence: An Indian Perspective, 17.2 UILS (2023) 114

[34] ibid

[35] ibid

[36] Duncan J Carter, AI Within Facilities Management: Expectations vs. Reality (2 January 2025, at 6:30 IST), [https://proptech.zone/ai-within-facilities-management-expectations-vs-reality/#:~:text="I think AI is coming, of more humanistic service jobs." &text=Artificial intelligence can take a, performance model and automate them.].

[37] Healthcare Challenges : Artificial Intelligence Promises Quantum Leap, 6.1 RSRR (2020) 182

[38] Digital Health in India - Key Trends and Impact of Regulation, 6.1 RSRR (2020) 1

[39] McKinney, S.M., et al. (2020) "International Evaluation of an AI system for breast cancer screening", Nature Medicine, 26(8), 1299-1308

By improving diagnosis accuracy, personalizing treatment plans, and streamlining administrative tasks, artificial intelligence (AI) has great promise for greatly enhancing patient care. A multifaceted approach is required to address these challenges. Building and maintaining patient trust is essential.

It was said that AI and digital health are considered to be futuristic, but after the covid 19 the digital health sector increased, and various models and trends created their own space in the healthcare sector. One of the biggest examples is e-pharmacies, which are commonly known as online pharmacies that deliver medicines through mail or courier. These apps allow pharmacies and companies to store the data of patients and after the update of AI in this app, the users get notifications and personal analysations regarding their medicines and health. In the advent of self-monitoring healthcare devices, these devices not only monitor but it also have sensors which make them a wearable technology, allowing to detect physiological changes in the body, the data which is collected enables to monitor and identify early symptoms of potential issues and receive timely alerts about the health.[40] After the introduction of electronic health records (EHRs) has also transformed healthcare by digitizing patient records. it eliminate the challenges associated with physical records such as loss and inaccessibility bu enablinh centralized storage that can be accessed anytime anywhere. However as these records and wearables genreate vast amount of data the concern of privany and data protection have become increasingly critical.[41]

It can be said that AI i.e. artificial intelligence is making significant inroads in the healthcare sector by utilizing complex algorithms and software to emulate human cognition in data analysis. They symbolize a plethora of combined innovations set to usher in a new category in health tech, from the personalisation sector to how everything will be enhanced by easy reach and the optimum realisation possible in terms of medical results. However, they equally underscore the significance of addressing ethical and regulatory challenges to maximize these benefits as much as possible.[42]

Data-handling capabilities and privacy risks associated with AI.

Artificial intelligence is revolutionizing the healthcare industry and is able to process big data quickly and effectively. AI is also working in the domain of artificial narrow intelligence (ANI) focusing on sectors like radiology, diagnostics, administration automation, etc. While the potential to evolve into AGI (artificial general intelligence) or ASI (artificial super intelligence) is phenomenal, we are still quite far from this and simply speculating.

AI's integration is not only about push but also pull factors since the push factors are large investments often funded by public, private, or philanthropic organizations. For instance, some of the ambitious initiatives in this direction have been taken by the Rockefeller Foundation. Aum has been kept for its Precision Public Health Initiative.[43]The ultimate expected outcome of all these investments is the more precise and economical practice of medicine. An Accenture study predicts that combining AI's efficiency with improved health outcomes could potentially save the healthcare industry around $150 billion by

[40] G. Appelboom, E. Camacho and M.E. Abraham, Smart wearable body sensors for patient self-assessment and monitoring, 72(1) Archives of Public Health (2014), available at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4166023/.

[41] L. Poissant, J. Pereira and R. Tamblyn, The Impact of Electronic Health Records on Time Efficiency of Physicians and Nurses: A Systematic Review, 12(5) Journal of the American Medical Informatics Association 505 (2005), 505, available at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1205599/.

[42] Healthcare Challenges : Artificial Intelligence Promises Quantum Leap, 6.1 RSRR (2020) 182

[43] World Health Organization. "Artificial Intelligence Is Changing the Health Sector." WHO Consultation Towards the Development of Guidance on Ethics and Governance of Artificial Intelligence for Health: Meeting Report Geneva, Switzerland, 2–4 October 2019. World Health Organization, 2021. http://www.jstor.org/stable/resrep35680.7.

2026. A further $150 billion in other savings would come through the adoption of AI tools and applications such as robot-assisted surgery, virtual nursing assistants for automated imaging diagnostics.[44]

As advancements in the healthcare sector, AI displays promise, but not without obstacles. The adoption of AI in the healthcare sector faces technical barriers, real limitation, or ethical dilemmas that pose delicate dilemmas or data security raisings. In addition, for AI to realise its potential, healthcare workers will have to learn new skills to work smoothly in combination with AI systems. Policy planners, engineers and clinicians will have to come together – in a conforming framework to address these challenges ensure safe, ethical, and useful uses of AI in healthcare.[45]

Legal and other challenges confronting AI in the healthcare industry.

1. **Data Privacy Concerns-** The Ministry of Health Care and Welfare introduced the EHR standards 2016 to regulate the management of electronic records[46] while focusing on the secure storage and sharing of health-related information. However, the privacy concerns remained a sensitive in the nature of health data; after certain exceptions, the recognized judgement of KS Puttuswamy it underscores an important stringent data protection measures, and After the bill of the DPDP act it mandates informed consent for using personal data and imposes strict penalties for breaches. In contrast, the bill permits certain exceptions for public health emergencies, such as during pandemic where the public interest lies over individual interest its prolonged deliberation has delayed implementation, leaving privacy concerns inadequately addressed.
2. **Risks in security and liability-** AI in healthcare is still a new concept, which make it open to cyberattacks and misuse which is present serious risk such as malware which can affect surgical robots or hospitals exploiting AI generated data for profit.[47] to safeguard or counter these issues robust security measures for AI is crucial whether it falls on developers, helathcare provders, or security firms and recognizing AI as a legal entity can also share accountablity among the stakeholders.
3. **Government Efforts-** For india, a country with the highest population, which means a country which holds the data of billions of people, it is necessary for the government to make necessary efforts to protect data and some of the introduced initiatives to support digitisation and AI adoption. The proposed National health authority aims to secure and strategize the health data.[48] In addition, the evidence for the use of AI comes from the AI Task Force and the policies of The Ministry of Electronics and Information Technology in Healthcare. Such an effort to deal with those will enable India to extract the full potential of AI and will ensure ethical and inclusive development within the sector.
4. **AI regulatory framework-** On a sectoral and large health scope, setting regulations would encompass regulation and comprehensive supervision of AI so that it is safe and ethically taken up. Advancing bodies such as the Drug Controller General of India and the Medical Council of India could become much more aware of the challenge that is at stake, namely health issues relating to servers as consequences of AI applications, extending this responsibility to looking into compliance with

[44] ibid.

[45] Healthcare Challenges : Artificial Intelligence Promises Quantum Leap, 6.1 RSRR (2020) 182

[46] *Report on Artificial Intelligence in the Healthcare Industry in India*, The Centre for Internet and Society, available at https://cis-india.org/internet-governance/files/ai-and- healtchare-report, last seen on 03/01/2025

[47] Diaz-Bone, R., Horvath, K., & Cappel, V. (2020). Social Research in Times of Big Data. The Challenges of New Data Worlds and the Need for a Sociology of Social Research. *Historical Social Research / Historische Sozialforschung*, *45*(3), 314–341. https://www.jstor.org/stable/26918415

[48] Healthcare Challenges : Artificial Intelligence Promises Quantum Leap, 6.1 RSRR (2020) 182

standardizations with due respect to safety and sensible dimensions of use.[49] Other interventions regarding the regulative framework could include the certification for either the national or state level, through which could develop more streamlined practices in changing the way in which care is received so that all kinds of health-related uses can be standardised using AI. This will help in helping trust and accountability in its use for AI applications.

5. **Intellectual Property Challenges-** Innovation areas for patents and copyright are sometimes very unusual for India, that most of the times they are not designed to work with the contemporary integrated styles of AI. In view of forthcoming further such development of AI, several moves, such as having an AI-specific clinic could be reforms introduced, and award-winning-maybe a prize or cash to push the sort of R&D action that is carried out on AI. For example, the interest to award IP in the first drug made by AI falls in this direction. AI-made works in the American conditions will end up being part of the public domain. Such would yield a better future for society as well.[50] The model has made room for India for confidentiality, which has given a clear edge not running the risk of having too valuable information blackout public and would in pay high cost due to people for any mere progress toward medicine development. Good IP refit would be anticipated as a crucial key since the infrastructure of who will own what is happening globally in the field of AI.[51]

Analysis of Informed Consent in the Context of Data Sharing and AI Use

Medical Ethics[52] and the Moral Obligations of Healthcare Professionals

Healthcare practice is based on medical ethics that are on the cornerstone of healthcare practice principles that define the moral obligations of healthcare professionals dedicated to patient care. Medical ethics at its core is benevolence, non malefice, autonomy and justice. These are healthcare providers principles in which we must place patients well being as a priority, avoid harm, respect individual autonomy and ensure equitable access to medical services.[53]

These ethics are founded in the concept of informed consent, as an expression of the moral and legal right patients have to decide autonomously about their treatment. [54]As artificial intelligence (AI) moves into the emerging phase of its evolution, informed consent has become not only an issue, but a multi pronged issue of its adequacy, implementation and ethical consideration in modern healthcare systems.[55]

The Traditional Health Care Concept of Informed Consent[56]

Traditionally this has been based on transparency and communication between healthcare provider and

[49] Danish Institute for International Studies. (2020). COVID-19: IMPACT AND INNOVATIVE RESPONSES. In *INNOVATIVE RESPONSES TO COVID-19: Future pathways for 'techvelopment 'and innovation* (pp. 9–28). Danish Institute for International Studies. http://www.jstor.org/stable/resrep27518.4

[50] *supra* n 35

[51] Healthcare Challenges : Artificial Intelligence Promises Quantum Leap, 6.1 RSRR (2020) 182

[52] Beauchamp TL and Childress JF, *Principles of Biomedical Ethics* (8th edn, Oxford University Press 2019)

[53] Mondal H and Mondal S, "Ethical and Social Issues Related to AI in Healthcare," *Methods in microbiology* (2024) <https://doi.org/10.1016/bs.mim.2024.05.009>

[54] Thomsen AC, Retanan LJ and Dubruel N, "GUIDANCE FOR INFORMED CONSENT IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE AND DATA VISITATION" [2024] AIDV Working Group DELIVERABLE 3 <https://www.rd-alliance.org/wp-content/uploads/2024/10/AIDV-WG-D3-Guidance-on-Informed-Consent-in-AIDV-2.pdf>

[55] Andreotta AJ, Kirkham N and Rizzi M, "AI, Big Data, and the Future of Consent" (2021) 37 AI & Society 1715 <https://doi.org/10.1007/s00146-021-01262-5>

[56] ibid

patients in the form of informed consent.[57] It requires that patients get straight, exact, and whole information about a diagnosis, possible remedies and expected medical risks and benefits. It enables people to take informed decisions in relation to their values and their preferences.

Legal precedents such as **Canterbury v. Spence (464 F.2d 772, D.C. Cir. 1972)** was that of the 'reasonable person' who should have been informed of the risks under the reasonable person standard.[58] The **Samira Kohli v Dr Prabha Manchanda (2008 2 SCC 1)** judgment marked the landmark judgment in India in reiterating the need for valid informed consent in light of the patient's right to autonomy.[59]

Informed Consent in the AI Era[60]

For example by launching AI health systems such as diagnostic tools and predictive analytics; new layer of complexity to informed consent is a reality. Because these systems often resemble "black boxes," with complicated algorithms, health care providers have difficulty articulating the rationale of AI generated recommendations. Systems such as these can understand the intentions of a developer, but it may be difficult for even developers to fully understand what these systems are doing. One example of this is probabilistic data that is used in imaging diagnostics, such as mammography screening, and hence may involve some communication uncertainties. AIs outputs, including risk scores which inherently differ from certainty complicate traditional notions of certainty in medical advice, and make it hard to tie an acceptable level of risk to informed consent.[61]

Data Privacy and Ownership Concerns

Up until now, healthcare has inherently been a data rich space, with massive datasets required for training and optimization of algorithm. Our reliance on consent raises questions about the extent of consent, since most patients consent to data use without fully understanding its meaning, in practice particularly for secondary uses including research or commercialization. Data governance is complicated by involvement of third parties and cross border data sharing, which may entrench the breaches of confidentiality.

It would seem that India's Personal Data Protection Act, 2023,[62] while not perfect, does provide addresses some of these concerns about patient data. Similar to GDPR, European Union's General Data Protection Regulation (GDPR) provides strict data protection framework and requires explanation before processing data. But the story of how Google DeepMind partnered with the UK's National Health Service (NHS)[63]

[57] " NCI Dictionary of Cancer Terms" (*Cancer.gov*) <https://www.cancer.gov/publications/dictionaries/cancer-terms/def/informed-consent>

[58] *Canterbury v Spence* 464 F.2d 772 (D.C. Cir. 1972)

[59] Samira Kohli v Dr Prabha Manchanda (2008) 2 SCC 1 (SC)

[60] Iserson KV, "Informed Consent for Artificial Intelligence in Emergency Medicine: A Practical Guide" (2023) 76 The American Journal of Emergency Medicine 225 <https://doi.org/10.1016/j.ajem.2023.11.022>

[61] Shah P and others, "Informed Consent" (*StatPearls - NCBI Bookshelf*, November 24, 2024) <https://www.ncbi.nlm.nih.gov/books/NBK430827/#:~:text=The%20function%20of%20informed%20consent,autonomous%20decisions%20about%20their%20care>

[62] The Digital Personal Data Protection Act 2023, Act No 22 of 2023 (India)

[63] UK House of Lords, 'AI in the UK: Ready, Willing and Able?' (HL Paper 100, 2018)

shows what can go wrong when the terms of data sharing agreements are unclear, so the need for strong regulation is highlighted.[64]

Ethical Foundations in Medical Practice[65]

The basis of medical practice is ethical responsibilities of the medical practice which depends on every interaction of healthcare professionals with the patient and the society. These responsibilities include:

1. Respect for Autonomy: Doctors must respect this right of patients to make informed decisions of care, free from coercive or undue influence.
2. Beneficence: Healthcare workers have ethical responsibility not only if they acted in the interest of their patients, but also initiate appropriate interventions to promote health and well being.
3. Non-Maleficence: A fundamental tenet: Patients are not supposed to be harmed, so decision making must be vigilant and best practice adherence must take place.
4. Justice: All pending for the provision of medical resources as well as treatments to people regardless of their demographic factors and socioeconomic basis.
5. Confidentiality: This reassures the patient during doctor-patient interaction and ethical obligation, legal requirement that protects the patient's information.

These principles are so broadly recognised around the world, they are contained in the Hippocratic Oath and in modern ethical codes such as the Declaration of Geneva.[66] One of the side of the Professional conduct, patient respect and continuous education is prominent in Indian area as per the Medical Council of India's Code of Ethics.[67]

Medical Negligence and Basis of Accountability

The area of medical negligence is still a key area of the confluence of ethics and law. The term for when a healthcare provider does not provide what should be expected, causing injury to the patient, is negligence. The Indian Medical Association v. V.P. Shantha (1995) 'Throwing medical services under the Consumer Protection Act, gave patients the right to seek redress of negligence.[68]

Healthcare professionals are required to observe established protocols, document all their actions and communicate well with the patients, the patient's families. Education in this area, including continuing education and peer consultations are essential to the making of an educated falling.

Enhancing Informed Consent in AI-Driven Healthcare[69]

Teaching patients more about AI in healthcare is the best way right now to get better informed consent. Using pictures, videos, and online tools that explain AI more simply helps patients learn enough to choose smart medical options. Both healthcare experts and patients need to understand AI better. Healthcare staff

[64] Hern A, 'Google's NHS Deal: Why Sharing Data with AI Is Raising Privacy Concerns' *The Guardian* (London, 1 May 2017)

[65] Gillon R, Philosophical Medical Ethics (John Wiley & Sons 1986)

[66] World Medical Association, 'Declaration of Geneva' (amended 2017)

[67] Medical Council of India, 'Code of Ethics Regulations, 2002'

[68] Indian Medical Association v. V.P. Shantha, (1995) 6 SCC 651 (SC)

[69] Park HJ, "Patient Perspectives on Informed Consent for Medical AI: A Web-Based Experiment" (2024) 10 Digital Health <https://doi.org/10.1177/20552076241247938>

need to learn how to explain AI technologies clearly. XAI technology helps both doctors and patients better understand how AI makes key healthcare decisions. With patient consent management tools, people get to choose what happens to their data and build stronger relationships based on honesty.[70]

Comparative Analysis of HIPAA and GDPR: Implications for Patient Data Protection in India

The rapid transformation of healthcare by technology has positioned patient data protection and security at the core of modern healthcare delivery. The rising implementation of advanced healthcare technology such as Artificial Intelligence (AI) across global nations demands strong data protection frameworks which safeguard both privacy and integrity of health information. Two major international standards for medical data protection exist through the Health Insurance Portability and Accountability Act (HIPAA)[71] in the United States and the General Data Protection Regulation (GDPR)[72] established by the European Union. As India experiences healthcare growth while adopting AI technologies it needs comprehensive understanding about how global frameworks affect and lead India's evolving legal rules specifically through Digital Personal Data Protection Act (DPDPA), 2023. A comparative analysis focuses on HIPAA and GDPR regulations to explain their direct importance for patient date security in India through a review of existing data privacy law frameworks.

Study of HIPAA in the Context of Privacy Safeguards

Introduced in 1996 by the United States: the Health Insurance Portability and Accountability Act (HIPAA) is a legendary legislative statute ensuring that patient information remains confidential in the health industry. The global standard for how to safeguard patient data, HIPAA requires full privacy and security standards to be met for sensitive patient data. Nation's such as India, trying to establish strong patient data protection frameworks, have been influenced by its principles.

HIPAA's framework has some important provisions. The Privacy Rule establishes national standards regarding the protection of individuals' medical records or other personal health information, and establishes criteria under which the information can be used or disclosed by covered entities, such as for treatment, payment or health care operations. Administrative, physical and technical safeguards are emphasized in the Security Rule to protect electronic PHI (ePHI) as well as to ensure that confidentiality, integrity and accessibility of ePHI are assured. The Breach Notification Rule requires notification both to affected individuals and to the appropriate authorities upon occurrence of a data breach, and the Enforcement Rule gives OCR the authority to investigate such breaches and to impose penalties for noncompliance.[73]

In contrast, India's recently passed Digital Personal Data Protection Act (DPDPA), 2023 covers healthcare data privacy via consent based data processing, accountability, and deep deterrent penalties for breach.

[70] Topol EJ, 'Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again' *Financial Times* (London, 15 March 2019)

[71] Health Insurance Portability and Accountability Act 1996, Pub L No 104-191, 110 Stat 1936 (US)

[72] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1

[73] Adams D, "Updating HIPAA Security to Respond to Artificial Intelligence" *Journal of AHIMA* (January 30, 2024) <https://journal.ahima.org/page/updating-hipaa-security-to-respond-to-artificial-intelligence>

This landmark Justice K.S. Puttaswamy v. Judgment in Union of India (2017) [74]made privacy fundamental right under the constitutional framework and heralded the route to privacy legislation. But India's structure is not comprehensive or unified like HIPAA, and this makes it difficult for India to work with cross borders data sharing and technology such as AI.[75]

HIPAA can teach India something about how a strong privacy framework should operate. Patient trust is enhanced by creating a unified approach for the protection of healthcare data, aiming for HIPAA's type of Privacy and Security Rules. To create a future ready healthcare privacy framework we need to embed enforceable mechanisms, breach notifications, safeguards for telemedicine and AI.

HIPAA serves to conclude, the complexities of contemporary healthcare provisions requires a global standard in addressing same, hence HIPAA. India's DPDPA is a major step forward but India can follow HIPAA's lead to strengthen privacy protections and maintain trust in a data driven healthcare ecosystem. In a landscape rapidly transforming, the ability to meet the challenges presented by emerging technologies and to protect patient information requires action.[76]

Examination of GDPR (General Data Protection Regulation)

The General Data Protection Regulation (GDPR) puts Europe at the forefront with a new legal framework implementing the protection of personal data. The comprehensive provisions allow for greater individual control of their data and accountability on organizations that handle sensitive data. GDPR has a major impact across the healthcare vertical where patient data is both most sensitive and is prone to misuse.[77]

Personal data as such is defined broadly in GDPR which includes any information that can identify directly or indirectly a person like medical records, genetic data and biometric data. Certain provisions specifically deal with how data about patients has to be very well protected. Specifically, Article 6 and Article 7 require that data processing be explicit and that consent has to be informed and that patients have the full control to withdraw consent. It also mandates data minimization that is, only data collection as necessary for a specific purpose to minimize the chances of breaches.

GDPR grants plenty of rights to the patients such as the following right to access, rectify or erase his or her data. Articles 24 – 30 highlight the importance of strong data security, i.e. encryption and pseudonymization – and they mandate that organizational compliance is documented. In addition, DPIAs are mandated for higher risk and uptake cases; identifying privacy implications from new health technologies.[78]

GDPR has created a benefit for the healthcare sector which relies heavily on sensitive patient data. It offers straightforward rules for managing electronic health records (EHRs), and supports global research through

[74] Justice K.S. Puttaswamy v Union of India (2017) 10 SCC 1 (SC)

[75] Rezaeikhonakdar D, "AI Chatbots and Challenges of HIPAA Compliance for AI Developers and Vendors" (2023) 51 The Journal of Law Medicine & Ethics 988 <https://pmc.ncbi.nlm.nih.gov/articles/PMC10937180/>

[76] Cohen IG, Mello MM, and Adashi EY, 'HIPAA and Protecting Health Information in the 21st Century' (2018) 320(3) *JAMA* 231 https://jamanetwork.com accessed 20 January 2025

[77] Abbasi J, 'GDPR and Its Impact on Healthcare Data Privacy' (2022) 5(6) *JAMIA* 543 https://academic.oup.com/jamia accessed 20 January 2025

[78] Kuner C, Bygrave LA, and Docksey C, The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020) https://global.oup.com accessed 20 January 2025

protection on cross national data sharing. GDPR places such things as telemedicine and artificial intelligence (AI) on the path of being accountable for ethical standards.

GDPR has influenced data protection laws in India, too, especially with the Digital Personal Data Protection Act (DPDPA), 2023 . The Indian act is based upon GDPR by making consent based processing and data subject rights a main integral for processing data in the country. But there are still gaps, for example, without DPIAs and reasonable cross border data transfer commitments. Aligning India's healthcare privacy framework with GDPR standards can happen by strengthening those areas.

Nevertheless, GDPR tends to face challenges. At times these requirements impede innovation in the field of medical research. For smaller healthcare Providers it could be difficult to meet this compliance costs, and to have global applicability is still a challenge since different countries have different international laws.

Thus, GDPR has defined a global bar for the protection of patient data, achieving the right balance between privacy and accountability. India's DPDP act includes some GDPR principles and some additional refinements are required to meet healthcare specific needs. Legal and ethical standards can be aligned to safeguard patient data and trust and innovation health care systems.

Suggestion & Conclusion

The adoption of AI technologies in healthcare has massive potential to change and accelerate in the future by mitigating medical practices, enhancing patient health, as well as improving the practice of it. Though this rapid advancement is no doubt a bargain to make, challenges come in the form of both guaranteeing patient data privacy and confidentiality. Indian legal framework exists but to solve the complexities and risks in AI driven healthcare there needs to be a new framework.

This result throws light on the need to improve in legal provision, informed consent, data security, and ethical guidelines so to guard tolerant patient sensitive information. The existing theories from international best practices, and inter disciplinary collaboration can bring the same knowledge to India to design a strong regulatory paradigm that is at the right equilibrium of privacy and accountability.

However, for this to work medical professionals cannot fail. As a matter of fact, they are the patient data custodians who have to adhere to ethical legal doctrines while utilizing AI to enhance healthcare delivery. However, if India can ensure, through comprehensive legal reforms supported by public awareness and ethical oversight, that the adoption of AI technologies in India's healthcare can not only change the sector but also ensure the fundamental rights of patients, India can guarantee that adoption of AI in healthcare in India can change the sector.

International frameworks like GDPR and HIPAA can teach us something from India. GDPR principles of data minimisation, purpose limitation and individual rights are all adaptable to Indian rules. Likewise, HIPAA's strong focus on protecting health information by way of the strongest of security measures can likewise inform the crafting of robust data protection standards.

There's a need to educate patients and healthcare providers about what AI means, what it could imply, and as importantly, share information about the importance of privacy of data. Public awareness campaigns can give people the ability to make the decision that's best for them when it comes to their data by educating and teaching their audiences on the information that is preserving and what the issues that are surrounding it.

India can, if addressed proactively, be the pioneer in the journey to harnessing the powers of AI to strengthen India's Healthcare ecosystem which is powered by the aspects of AI with respect to privacy, dignity and trust.