



Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Evaluating the Legal Framework and Challenges of Telemedicine in India: Privacy, Liability, and Regulatory Compliance

Saesha Bhalla^a

^aCHRIST (Deemed to be University), Bangalore, Central Campus, India

Received 17 December 2024; *Accepted* 18 January 2025; *Published* 22 January 2025

Telemedicine, also known as digital healthcare, is a means to attain healthcare consultation and services via digital platforms, and it has become a transformative force in India, particularly after the introduction of the Telemedicine Practice Guidelines¹. The guidelines provided ensure healthcare accessibility, recognise telemedicine as a progressing and emerging field and regulate the responsibilities of registered medical practitioners as defined within the guidelines issued by the Ministry of Health and Family. Despite the potential of telemedicine as an emerging field, the practice faces significant legal and ethical challenges. Although these guidelines provide instructions to ensure the protection of all the parties involved while availing of telemedical services, certain concerns arise through the development in this industry, which are often negated. The key concerns include patient privacy, medical liability, and regulatory compliance. Although the guidelines are read with the Information Technology Act of 2000² and the Personal Data Protection Bill³ can offer some safeguards, data breaches and cybersecurity risks remain a pressing concern due to the lack of specific legislation.

¹ 'Telemedicine Practice Guidelines, 2020' (Ministry of Health and Family Welfare, 25 March 2020) <https://esanjeevani.mohfw.gov.in/assets/guidelines/Telemedicine_Practice_Guidelines.pdf> accessed 15 October 2024

² Information Technology Act 2000

³ Digital Personal Data Protection Act 2023

Furthermore, telemedicine platforms often involve third-party entities or platforms, and the guidelines are silent on determining liability in medical negligence cases. While the future of telemedicine in India looks promising, overcoming challenges related to privacy, infrastructure, and patient trust is essential for its sustained growth. This paper analyses the legal framework governing telemedicine in India, focusing on privacy protection, liability, and the lapses in the guidelines issued for telemedicine.

Keywords: *accountability, data protection, liability, privacy, telemedicine.*

INTRODUCTION

Telemedicine is also known as E-medicine or digital healthcare. This approach provides health services from a distance using tech for communication (Voice, Audio, Text, & Digital Data exchange) and has become more popular in India. It allows patients to seek medical advice, diagnoses, and care without physically going to a doctor and using other tech means, and it increases accessibility and is cost-efficient.⁴ India is a diverse country with a huge population, and the doctor-patient ratio is insufficient. As technology advances, telemedicine helps more people get care in rural areas or places with few doctors. It also takes some pressure off the regular healthcare system.

The Indian government and medical authorities have recognised its potential, leading to the formulation of policies that support its expansion. Although some states like Karnataka have banned telemedicine facilities, the Karnataka Medical Council warned practitioners that such practices are illegal⁵ through the introduction of Telemedicine Guidelines by the Ministry of Health and Family Welfare.

The 'Telemedicine Practice Guidelines,' which are included in Appendix 5 of the Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulation, 2002,⁶ provide a structured framework for telemedicine in India. Established in 2020, these guidelines offer healthcare professionals clear directives on how to deliver care through digital means. As telemedicine

⁴ ACM Fong et al., *Telemedicine Technologies: Information Technologies in Medicine and Telehealth* (John Wiley & Sons Ltd 2010)

⁵ Afshan Yasmeen, 'KMC warns doctors against online consultations' *The Hindu* (Bengaluru, 14 May 2019) <<https://www.thehindu.com/news/national/karnataka/kmc-warns-doctors-against-online-consultations/article27130640.ece>> accessed 24 October 2024

⁶ Fong (n 1)

continues to evolve, it is anticipated to play a vital role in transforming India's healthcare ecosystem. The growth of telemedicine in India has been driven by several factors, including advancements in technology, increased internet penetration, and the rising demand for healthcare services. The COVID-19 pandemic, in particular, acted as a catalyst for telemedicine adoption, as lockdowns and social distancing norms made physical consultations difficult.

The Indian government's proactive stance on promoting digital health also played a key role in the expansion of telemedicine. Initiatives such as the National Digital Health Mission (NDHM) and the Ayushman Bharat scheme have integrated telemedicine into broader healthcare reforms.⁷ With the growth of Private healthcare providers, startups and tech companies have contributed to the rapid growth of telemedicine services by developing user-friendly platforms and mobile apps that facilitate remote consultations.⁸

Despite challenges related to infrastructure, digital literacy, and regulatory compliance, telemedicine is increasingly becoming a viable and popular mode of healthcare delivery across India, particularly in rural areas where access to healthcare professionals is limited. The future of telemedicine in India looks promising, with ongoing efforts to address legal, privacy, and technical concerns.⁹

LEGAL FRAMEWORK GOVERNING TELEMEDICINE & REGULATORY COMPLIANCE FOR TELEMEDICINE SERVICES IN INDIA

The legal perspective in India has quite a few regulations in place to provide a legal basis for healthcare delivery through digital means. It was the Telemedicine Practice Guidelines, 2020,¹⁰ that was the breakthrough aimed at teleservices unification to provide digital health care. The guidelines not only provide a safe, private, and informed patient consent-based framework for

⁷ Simrin Sirur, 'Younger and female doctors adopted telemedicine more during Covid in India, study says' *The Print* (New Delhi, 05 October 2020) <<https://theprint.in/health/younger-and-female-doctors-adopted-telemedicine-more-during-covid-in-india-study-says/516833/>> accessed 24 October 2024

⁸ 'India's new Telemedicine Practice Guidelines – Analysis and Do's and Don'ts for Doctors offering Teleconsultation' (*Arogya Legal*) <<https://arogyalegal.com/2020/article/indias-new-telemedicine-practice-guidelines-analysis-and-dos-and-donts-for-doctors-offering-teleconsultation/>> accessed 24 October 2024

⁹ Sunny Parayan, 'Telemedicine in India: Transforming Healthcare Accessibility and Delivery' (*Medicircle*, 04 August 2023) <<https://medicircle.in/telemedicine-in-india-transforming-healthcare-accessibility-and-delivery>> accessed 24 October 2024

¹⁰ Telemedicine Practice Guidelines, 2020 (n 1)

the registered medical practitioner (RMP) but also provide a clear protocol for remoting healthcare services. Other relevant legislations include the Drugs and Cosmetics Act of 1940, which regulates the sale of drugs through e-pharmacies, and the Clinical Establishments Act of 2010,¹¹ which mandates healthcare establishments to maintain digital records for transparency and uniformity in healthcare delivery, although they are not directly applicable but can be interpreted for the ensuring digital healthcare.¹²

The Telemedicine Practice Guidelines 2020¹³ give complete instructions on how to deliver healthcare through telemedicine. They stress patient rights and what doctors must do. These rules cover many things, such as getting clear or implied consent from patients using telemedicine in different health situations and keeping digital communication private. One of the essentials that the guidelines provide is that getting informed consent is key.¹⁴ Patients who can communicate their consent must provide express consent, whereas when patients are unable to provide express consent, implied consent can be taken into consideration, provided in another case, it has to be clear consent. The rules also talk about keeping records, writing prescriptions, and when doctors should see patients face-to-face. This is a step to prevent misdiagnoses and illegal prescriptions.

The Information Technology Act 2000¹⁵ is a crucial legislation for telemedicine and its governance in India. It controls how health data moves. The IT Act describes sensitive personal data. This includes health records. It says platforms that handle this kind of data need protection. The Act sees telemedicine platforms as middlemen. This means they must follow legal rules for storing data, privacy policies, and getting consent. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011¹⁶ make this more stringent. They set rules for handling health data.

¹¹ Clinical Establishments (Registration and Regulation) Act 2010

¹² Drugs and Cosmetics Act 1940

¹³ Telemedicine Practice Guidelines, 2020 (n 1)

¹⁴ Ministry of Health and Family Welfare, 'A big win for Digital India: Health Ministry's 'eSanjeevani' telemedicine service records 2 lakh tele-consultations' (*Press Information Bureau*, 19 August 2020) <<https://pib.gov.in/PressReleasePage.aspx?PRID=1646913>> accessed 26 September 2024

¹⁵ Information Technology Act 2000

¹⁶ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

CONCERNS WITH TELEMEDICINE AS AN EMERGING FIELD IN INDIA

The Telemedicine Practice Guidelines 2020¹⁷ of India were essential in regulating telemedicine services in the country. However, despite this, the legal doubts still hinder the process. The guidelines deal with the issues faced by registered medical practitioners but do not address the legal side that is affected, mainly in terms of privacy and liability. Telemedicine includes the handling of particularly sensitive personal data, such as health records, which are under the Information Technology Act 2000¹⁸ and the related Data Protection Rules 2011¹⁹. The absence of a comprehensive data protection law in India leads to privacy invasions of patients, as proven by the recent cyberattacks on healthcare institutions.²⁰

The next legal challenge is about responsibility. The majority of telemedicine cases involve consultations and treatment provided and managed worldwide, stirring some responsible and accountability questions about these healthcare providers. Legal disputes are more likely to happen in case of any complication appearing during teleconsultations, especially across state or national borders. The present framework is handicapped by the lack of clarity in the definition of the responsibilities of healthcare providers in such scenarios, thus creating difficulty in fixing liability in cases of medical negligence.

PRIVACY CONCERNS IN TELEMEDICINE

The quick growth of telemedicine has made healthcare more accessible in remote places. This progress, though, has created privacy issues when it comes to handling sensitive patient information. To protect patient privacy while using digital platforms for healthcare, we need to set up stringent laws and follow regulations.

¹⁷ Telemedicine Practice Guidelines, 2020 (n 1)

¹⁸ *Ibid*

¹⁹ Clinical Establishments (Registration and Regulation) Act 2010

²⁰ 'Indian healthcare sector faces 6,953 cyberattacks weekly, outpacing global rates: Check Point threat intelligence report' (*Express Computer*, 28 June 2024) <<https://www.expresscomputer.in/news/indian-healthcare-sector-faces-6953-cyberattacks-weekly-outpacing-global-rates-check-point-threat-intelligence-report/113528>> accessed 26 September 2024

Privacy concerns in telemedicine stem from issues related to data protection and confidentiality, as well as the introduction of the Personal Data Protection Bill²¹. Safeguarding sensitive patient information is crucial in telemedicine, especially as consultations and medical records are more frequently stored and shared electronically and should uphold the same standard as physical consultations. The IT Act defines sensitive personal data to include details about health conditions, medical history, and biometric information. The Act, coupled with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011²², mandates that telemedicine platforms adopt stringent security measures to protect this information.

Telemedicine platforms, which act as intermediaries under the IT Act, are required to implement reasonable security practices, such as encryption and secure data transmission, to safeguard patient data from breaches.²³

Even though these measures exist, the Institute of Medical Sciences (AIIMS), which compromised sensitive patient data, showed the vulnerabilities in India's healthcare infrastructure as well as how there can be a breach caused by the absence of laws protecting the medical data of patients.²⁴

The Telemedicine Practice Guidelines 2020²⁵ recognises the significance of data protection, mandating registered medical practitioners to maintain the confidentiality of patient records during teleconsultations, and the guidelines require RMPs to secure explicit consent from

²¹ Trishaljeet Singh and Sumit Kaushik, 'Digital Personal Data Protection Act (DPDP Act), 2023' (*Lawrbit*, 22 November 2022) <<https://www.lawrbit.com/article/digital-personal-data-protection-bill-2022/>> accessed 20 June 2024

²² *Ibid*

²³ Luv K Sharma and Meena Rajput, 'telemedicine: socio-ethical considerations in the Indian milieu' (2009) 77(2) *Medico-Legal Journal* <https://www.researchgate.net/publication/26790595_Telemedicine_Socio-Ethical_Considerations_in_the_Indian_Milieu> accessed 24 June 2024

²⁴ 'AIIMS Delhi cyber attack: 5 main servers hacked, China suspected to be involved' (*Business Today*, 02 December 2022) <<https://www.businesstoday.in/latest/trends/story/aiims-delhi-cyber-attack-5-main-servers-hacked-china-suspected-to-be-involved-355099-2022-12-02>> accessed 24 July 2024

²⁵ Telemedicine Practice Guidelines, 2020 (n 1)

patients before sharing any personal health information with third parties, strengthening the principle of confidentiality in telemedicine practices.²⁶

Despite regulations for privacy protection in the guidelines and the IT Act, ambiguity remains regarding rules addressing certain privacy concerns. The absence of comprehensive legislation covering data protection specific to telemedicine leaves patients vulnerable to data misuse, especially in the face of emerging cyber threats²⁷. Additionally, while the guidelines focus on medical practices, they do not address broader legal aspects such as cross-border consultations, jurisdiction, and enforcement of accountability, which are critical due to the involvement of various stakeholders and platforms in telemedicine.

The guidelines lack specific enforcement mechanisms, which raises concerns about the mishandling of patient health data due to insufficient cybersecurity measures, which shows that telemedicine platforms do not adhere to the highest security standards as of now. The absence of accountability for privacy violations only worsens the situation. While the forthcoming Privacy bill aims to regulate sensitive personal data, such as health records, its delayed approval continues to threaten patient privacy.

In the digital healthcare landscape, communication frequently involves third-party platforms that are not held accountable under these guidelines. The participation of various entities, including telemedicine platforms, insurance companies, and pharmacies, increases the risk of unauthorised data sharing, heightening the chances of privacy breaches. Unfortunately, these potential breaches resulting from third-party involvement have not been adequately addressed in the telemedicine guidelines, which could lead to significant privacy violations.

COMPLIANCE WITH THE PERSONAL DATA PROTECTION BILL

The proposed Personal Data Protection (PDP) Bill²⁸ aims to establish a comprehensive framework for data protection in India, encompassing all sectors, including healthcare. The bill

²⁶ Chae Canon, 'Is Your Practice HIPAA Compliant' (*OptimisPT*, 13 December 2023) <<https://optimispt.com/is-your-outpatient-physical-therapy-practice-hipaa-compliant/>> accessed 08 October 2024

²⁷ Kausik Lahiri, 'Telemedicine, e-Health and Health related IT enabled Services: the Indian Situation' (2013) 7 *Globsyn Management Journal* <https://www.researchgate.net/publication/305021078_Telemedicine_e-Health_and_Health_related_IT_enabled_Services_the_Indian_Situation> accessed 08 October 2024

²⁸ Singh (n 21)

categorizes health data as 'sensitive personal data' and mandates explicit patient consent before any entity can collect, process, or share such data.²⁹ Telemedicine platforms will be required to comply with the bill's provisions, which also include limitations on data processing by third parties and requirements for data localisation, necessitating the storage of sensitive data within the country.³⁰

PDP Bill's main provision is the necessity for informed consent, mainly in the context of telemedicine. On a related note, patients are supposed to be fully informed about the potential use of their data and be allowed to decompose on any condition that can be overwritten. Furthermore, e-healthcare providers and telemedicine platforms must ensure that the data is used only for the purpose for which the consent was given. Besides, concerns existed that the government was supposed to be the principal actor in case the policy was applied that would have the product cause the same (Open System Interconnection) OSI problem as the case where the product is used in the cloud. The government then would be liable for abuse of health data without the presence of a conducting officer who ensures the usage's legitimacy with the misuse of health data without proper oversight.

LEGAL LIABILITIES IN TELEMEDICINE PRACTICES

Telemedicine has revolutionised healthcare, but it has also brought about complexities in terms of medical negligence and legal responsibilities.³¹ Negligence in telemedicine is on the same legal footing as in traditional healthcare services. It is governed by the principles of tort law that have been in force since 1986 and those of the Consumer Protection Act 1986. Regardless of this, telemedicine brings a unique element of proving negligence, for example, in cross-border or virtual consultations and the provision of care by a distant physician. The required quality of care for doctors and traditional doctors must be identical. A medical practitioner who does not

²⁹ 'Data Protection and Cybersecurity Developments 2023' (*In-House Community*, 09 May 2023) <<https://www.inhousecommunity.com/article/data-protection-cybersecurity-developments-2023/>> accessed 08 October 2024

³⁰ Christopher C Gillman-Wells et al., 'COVID-19 Reducing the Risks: Telemedicine is the New Norm for Surgical Consultations and Communications' (2020) 45(1) *Aesthetic Plastic Surgery* <<https://pmc.ncbi.nlm.nih.gov/articles/PMC7471549/>> accessed 08 October 2024

³¹ Saroj Kanta Mishra et al., 'Telemedicine in India: current scenario and the future' (2009) 15(6) *Telemedicine & e-Health* <<https://pubmed.ncbi.nlm.nih.gov/19659413/>> accessed 08 October 2024

reach this standard, whether it be through misdiagnosis or incorrect treatment through telemedicine, might be held accountable for negligence.³²

The Telemedicine Practice Guidelines³³ are the guidelines that were established to guide RMPs (Registered Medical Practitioners) on how teleconsultations should be carried out, including the rules for the treatment, consent, and data management that they have to follow. The guidelines are clear that RMPs must judge if a teleconsultation is suitable, and then they should recommend an alternative in case it's not suitable. The mistake of not duly examining and treating a patient via telemedicine could cause the practitioner to be accused of malpractice by the patient.³⁴ In addition to that, the loss of physical examination in teleconsultations would make it more difficult for the healthcare provider to ensure the duty of care for the patient.

Liability risks faced by healthcare providers and liabilities incurred due to miscommunication, wrong diagnoses, and using the patient database incorrectly have become a part of telemedicine these days. The very purpose of the IT Act is to regulate the process of health data exchange and ensure the safe storage of patients' records. Intermediaries categorised under the IT Act as telemedicine applications should respect data protection regulations to avoid liabilities due to privacy breaches. Nevertheless, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011 strengthen the healthcare providers' duties to the data protection of their patients³⁵. Non-compliance with the said rules may lead to legal action under the IT Act. Also, they encounter the intricacies of trans-border care, more so when the patient is located in another state or a different country. Issues of legal jurisdiction and responsibility become more circuitous in these circumstances, particularly in the different healthcare laws across the territories. As of now, the Indian courts have not provided much guidance on the adjudication of telemedicine disputes, even if this is likely to develop as the practice becomes more popular. In India, the jurisprudence concerning telemedicine liabilities is still in the developmental stage. The Indian judicial system has not yet heard numerous cases of medical negligence and liability that are specific to telemedicine.

³² Navneet Ateriya et al., 'Telemedicine and virtual consultation: The Indian perspective' (2018) 31(4) National Medical Journal of India <<https://doi.org/10.4103/0970-258X.258220>> accessed 08 October 2024

³³ Telemedicine Practice Guidelines, 2020 (n 1)

³⁴ Gillman-Wells (n 30)

³⁵ *Ibid*

However, the growing worldwide jurisprudence offers guidance on how Indian courts may handle such disputes in the future. For instance, the case of *Dr. Christian Hageseth v People in the US*,³⁶ where a psychiatrist was found in breach of law under California jurisdiction, although the prescribed medication had been given online by another state, is a model that the Indian courts might want to consider. There could be similar decisions in India if telemedicine services get cross-border, which will be more frequent in the future.

Moreover, in the case of telemedicine, one of the main issues is the fact that there is usually more than one healthcare provider involved. Therefore, establishing the party accountable for a certain aspect of the patient's care may create complications that the party may have to deal with when it comes to legal liability. The non-unitary form of telemedicine solutions means that a situation may arise where first-level care will be done by one doctor and then specialist care by another one, leading to disputes about which one is going to be the one taking responsibility in case of negligence. Hospitals and other healthcare institutions can implement telemedicine in a variety of ways. What is consistent, however, is that it usually is a quality standard among healthcare providers. To mitigate the above-mentioned issues, the courts must come up with clear and shared liability allocation among the healthcare providers who work through the medical teleconsultation platforms.

The instructions are not exhaustive of the telemedicine legal liability, *inter alia*, involving healthcare providers from other jurisdictions (state or country). This may be the principal factor in the resolution of disputes in cases of negligence.³⁷ A core aspect of telemedicine is that several healthcare professionals are involved in the delivery of treatments, which will make it difficult to define the exact person who will be responsible and liable. Telemedicine guidelines still do not make clear the exact distribution of responsibility between the primary care provider, specialists, and the platform provider. The instructions require RMPs to use their knowledge when taking up teleconsultations, but they offer only some direct instructions on the possible

³⁶ *Dr Christian Hageseth v People* [2016] COA 78 (Colo Ct App 2016)

³⁷ Jitender Aneja and Sonam Arora, 'Telemedicine and ethics: opportunities in India' (2021) 6(4) *Indian Journal of Medical Ethics* <[https://ijme.in/articles/telemedicine-and-ethics-opportunities-in-india/?galley=html#:~:text=Introduction,of%20Andhra%20Pradesh%20\(1\)](https://ijme.in/articles/telemedicine-and-ethics-opportunities-in-india/?galley=html#:~:text=Introduction,of%20Andhra%20Pradesh%20(1),)> accessed 30 October 2024

accountability if perhaps there is a wrong diagnosis or if no physical examination is done.³⁸ The matter of healthcare professionals' liable behaviour in telemedicine is rather serious, being that the legal framework of such an issue is still at the stage of an ongoing elaborative process.

PATIENT TRUST AND ACCEPTANCE

Patient Trust and acceptance play a crucial role when it comes to adopting telemedicine, and the lack of clarity in certain aspects relating to data privacy and liability poses a significant barrier in the same. The lack of benefits, rights and protection could lead to a sense of distrust or hesitation in availing telemedicine services, especially in rural areas where healthcare facilities like this could substantially improve living conditions.³⁹ The lack of awareness about the benefits and safety of telemedicine exacerbates the issue. Cultural and social factors influence health-seeking behaviour, with patients often preferring traditional healthcare systems over formal telemedicine platforms.⁴⁰

Data privacy is yet another crucial aspect of patient trust. Patients are often worried about the confidentiality of their medical information, especially in light of increasing reports of data breaches and the absence of strong legal protections for digital health data⁴¹. The lack of clarity around informed consent in telemedicine consultations further undermines patient confidence. While the Telemedicine Practice Guidelines 2020 mandate explicit consent for certain procedures, many patients are unaware of their rights, leaving them vulnerable to the misuse of their data.⁴²

Although the guidelines require informed consent, particularly for data sharing, many patients lack the digital literacy to comprehend the implications of telemedicine. This can lead to patients giving partial consent and unwillingly agreeing to terms that may compromise their privacy.

³⁸ Dipika Jain, 'Regulation of Digital Healthcare in India: Ethical and Legal Challenges' (2023) 11(6) Healthcare <<https://doi.org/10.3390/healthcare11060911>> accessed 30 October 2024

³⁹ Sirur (n 7)

⁴⁰ Rajesh K Chandwani and Yogesh K Dwivedi, 'Telemedicine in India: current state, challenges and opportunities' (2015) 9(4) Transforming Government: People, Process and Policy <<https://www.emerald.com/insight/content/doi/10.1108/tg-07-2015-0029/full/html>> accessed 30 October 2024

⁴¹ Aneja (n 37)

⁴² Telemedicine Practice Guidelines, 2020 (n 1)

According to the telemedicine guideline, the differentiation between implied and explicit consent can confuse, leading to patients waiving their rights unknowingly, which could lead to hesitation in availing of these services.

CONCLUSION AND RECOMMENDATIONS

Telemedicine is a transformative and emerging field in India with exponential prospects and is a tool to bridge the gap between urban and rural healthcare access and provide advanced and better medical facilities to a larger consumer group. The Telemedicine Guidelines, read with other relevant laws related to telecommunication and data protection, recognise and regulate this emerging sector. Although these guidelines have provided much clarity for healthcare professionals as well as patients' rights. However, despite these existing regulatory compliances, there is much room for potential breach of patient rights, and there exist several challenges, particularly in areas concerning privacy, liability and regulatory compliances.

There is a lack of appropriate framework or regulations that deal with these potential breaches since the liability and guidelines, although relevant, are arbitrary or silent on some crucial aspects which could arise out of the process of availing digital healthcare. Current laws and regulations, namely the Information Technology Act of 2000 and the Personal Data Protection Bill, aim to tackle the complexities of data protection and also include medical records within their ambit of personal data, but these frameworks remain fragmented and undeveloped when dealing with the niche nature of digital healthcare. Also, the legal uncertainties regarding medical negligence and the lack of clear jurisdictional guidelines present a significant barrier to adopting telemedicine.

Comprehensive regulatory reforms and codes should be introduced, which could further the potential of telemedicine in India and enable this emerging field to utilise its fullest potential. Additionally, investing in technological infrastructure and enhancing digital literacy, particularly in rural areas, will be crucial to ensuring equitable access to telemedicine. By drawing lessons from global best practices and implementing targeted reforms, India can establish a more secure and effective telemedicine ecosystem that serves both urban and rural

populations. With the right regulatory and technological support, telemedicine can become a key driver in achieving India's healthcare goals.