BRIDGING THE DIVIDE: A TECHNO-MEDICO-LEGAL ANALYSIS OF TELEMEDICINE AND VIRTUAL HEALTHCARE REGULATION IN INDIA

Deepikka R S, Junior Research Fellow, Research Scholar, School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Chennai.

ABSTRACT

The rapid digitisation of healthcare delivery in India, accelerated by the COVID-19 pandemic and institutionalised through the Ayushman Bharat Digital Mission, has created a regulatory vacuum at the intersection of three traditionally distinct disciplines, namely law, technology and medicine. As Telemedicine and e-health have transformed into an inevitable component of clinical practice, the statutory architecture that governs them still remains fragmented across various laws like the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, various Telemedicine Practise Guidelines and other professional guidelines issued by the state and national medical councils, etc that were never drafted with the interplay between law, technology and healthcare in mind. Innumerable cyber-attacks on the healthcare systems, breach of patient's data privacy and confidentiality, role of Artificial Intelligence in healthcare systems, evolution of new virtual healthcare devices and practices have exposed the vulnerabilities of the Indian healthcare system that is racing towards digitisation without an optimal legal safety net. This paper undertakes a techno-medico-legal analysis of the Indian regulatory landscape governing telemedicine, e-health and cybersecurity in the healthcare sector. It maps the individual statutory regimes that touch upon law, technology and healthcare, identifies the precise points at which these regimes intersect and, at times, contradict one another, and situates the Indian position within a comparative framework alongside the United States and the United Kingdom. The paper concludes with a set of concrete legislative and institutional recommendations and argues that interdisciplinary research on techno-medico-legal scholarship is no longer an academic luxury but a basic necessity for safeguarding the health data and physical wellbeing of Indian citizens.

Keywords: Telemedicine; E-Health; Virtual Healthcare; Health Data; Cybercrime; Techno-medico-legal.

I. INTRODUCTION

For much of legal history, medicine and law developed along parallel tracks that intersected only occasionally in the courtroom, say in a malpractice suit, or in the framing of a licensing statute. In this equation Technology was a mere side actor with more focus on the medical jurisprudence, but that era has ended. With the advent of e-health and telemedicine a patient from any remote part of India may receive a diagnosis from a specialist sitting in a city, transmitted through a video link, recorded on a cloud server owned by a private company, and billed through a payment gateway regulated by yet another statute. In this single transaction, medicine, technology and law are no longer parallel, they are entangled. The Government of India's own flagship digital health initiative, the Ayushman Bharat Digital Mission, envisions a unique health identity for every citizen, interoperable electronic health records, and a registry of doctors and health facilities, all built on a shared digital public infrastructure.[1]

It is this entanglement of the three previously distinctly studied disciplines, that this paper calls the techno-medico-legal problem. The problem is not new in kind, but it is new in scale and urgency. The Telemedicine Practice Guidelines, 2020, issued in the early days of the COVID-19 pandemic, were a hurried but necessary legal response to a medical crisis that technology alone had made survivable.[2] Three years later, the Digital Personal Data Protection Act, 2023[3], arrived as India's first comprehensive data protection statute, yet it was drafted with only a passing regard for the peculiar sensitivity of health information. Between these two moments sits a governance gap that this paper seeks to close.

The purpose of this article is to demonstrate why law, technology and medicine can no longer be studied or legislated upon in isolation but needs dedicated research to develop effective regulatory mechanisms that individually and jointly govern this space and protect the digital rights and health rights of all Indian citizens.

[1]Ministry of Health and Family Welfare, Government of India, *Ayushman Bharat Digital Mission* (National Health Authority, 2021), available at https://abdm.gov.in (last visited 10 July 2026).
[2]Board of Governors, Medical Council of India, *Telemedicine Practice Guidelines*, Ministry of Health and Family Welfare, Government of India (25 March 2020), Appendix 5 to the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.
[3] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India). But at present only the foundational principles of the act are in force and other rules like implementation of consent managers and other compliance obligations are being implemented in a phased manner between November 2026 and May, 2027.

II. THE RISE OF TELEMEDICINE AND E-HEALTH IN INDIA

India's engagement with telemedicine did not begin with the pandemic, but it was the pandemic that transformed a niche practice into a mainstream mode of healthcare delivery. Prior to 2020, telemedicine existed in a legal grey zone. the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, were silent on remote consultation, leaving registered medical practitioners exposed to disciplinary and even criminal liability for prescribing medicine without a physical examination.[4] The Board of Governors of the erstwhile Medical Council of India resolved this uncertainty by notifying the Telemedicine Practice Guidelines as Appendix 5 to the 2002 Regulations, thereby legitimising teleconsultation, defining permissible modes of communication, and prescribing a tiered system for the categories of medicines that may be prescribed remotely.

The scale of adoption that followed has been extraordinary. The National Digital Health Blueprint, released in 2019, laid the architectural foundation for what would later become the Ayushman Bharat Digital Mission, envisaging a federated system of health data that could be accessed, with consent, across public and private providers.[5] The Government's own teleconsultation platform, eSanjeevani, has reported crossing over forty five crore consultations, (as on July,2026) making it one of the largest publicly operated telemedicine networks in the world.[6]

The World Health Organization has long recognised e-health, defined broadly as the use of information and communication technology for health, as central to achieving universal health coverage in resource-constrained settings, a description that fits India's vast rural-urban healthcare divide with particular force.[7] Yet adoption has consistently outpaced regulation. Electronic health records, wearable health devices, artificial intelligence-assisted diagnostic tools and e-pharmacies have all entered clinical practice in India well before any statute was drafted with their specific risks in mind, a pattern that recurs throughout this paper and that lies at the heart of the case for interdisciplinary legal research.

[4]Latika Vashist, "Regulating Telemedicine in India: A Critical Appraisal", 61 *Journal of the Indian Law Institute* 205, 210 (2019).
[5]Ministry of Health and Family Welfare, *National Digital Health Blueprint* (2019), paras 3.1-3.4.
[6]E-sanjeevani, available at https://esanjeevani.mohfw.gov.in/#/(last visited 10July 2026).
[7]World Health Organization, *Global Diffusion of eHealth: Making Universal Health Coverage Achievable* (WHO, Geneva, 2016) 9-14.

III. CYBERCRIME AND CYBERSECURITY CHALLENGES IN INDIAN HEALTHCARE

Although the digitisation of in healthcare industry has brought immeasurable benefits to the public health and access to healthcare to patients, such benefits have also been shadowed by numerous attacks by cybercriminals, targeting patients data, hospital infrastructure, national security etc. for cybercriminals healthcare data is a uniquely attractive target which hold financially valuable and highly sensitive data, they cannot easily suspend operations without endangering life, and, in India particularly, their information technology infrastructure has historically been under-resourced relative to the volume of data it carries. This vulnerability was exploited as demonstrated on 23 November 2022, when the servers of the All-India Institute of Medical Sciences, New Delhi, one of the country's most prestigious public hospitals, were crippled by a ransomware attack that forced the institution into weeks of manual, paper-based operation across its emergency, outpatient, inpatient and laboratory services.[8]

The Indian Computer Emergency Response Team indicated that the attackers had compromised the physical and virtual servers and that the personal and medical data of an estimated forty million patients, may have been exposed.[9] The incident was significant not merely for its scale but also for its legal characterisation. The Delhi Police's registered the matter as one of cyber terrorism and extortion under section 66F of the Information Technology Act, 2000, a provision ordinarily reserved for threats to the sovereignty and integrity of the nation, reflecting the gravity of an attack on critical healthcare infrastructure. This incident has exposed not only a technical vulnerability but a legal one, namely at the time of the attack, India had no dedicated health data protection statute, and even the Digital Personal Data Protection Act, enacted the following year, does not create a distinct, heightened category for health information of the kind that existed under the erstwhile The Information Technology (reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011.[10]

[8]Ransomware Attack on the All-India Institute of Medical Sciences, New Delhi (23 November 2022); see Lok Sabha Unstarred Question No. 3021, answered on 16 December 2022, Ministry of Health and Family Welfare.
[9]Indian Computer Emergency Response Team (CERT-In), *India Ransomware Report 2022*, available at https://www.cert-in.org.in (last visited 10 July 2026).
[10]"The AIIMS Cyber-Attack and India's Dilapidated Cyber-Security Infrastructure", NLIU Centre for Studies in Intellectual Property Rights (2023).

AIIMS is illustrative rather than exceptional. Smaller nursing homes, government and private telemedicine platforms, e-health apps, diagnostic laboratories and e-pharmacy platforms, also handle equally sensitive data but operate with a fraction of AIIMS's resources, making it more exposed. The consequence of a breach in a healthcare setting is also qualitatively different from a breach in a purely commercial one as compromised medical records cannot be reissued in the way a stolen credit card number can be cancelled and replaced, and a denial-of-service attack on hospital systems can directly imperil patient safety rather than merely inconvenience a consumer.[11] It is this coupling of technological vulnerability with irreversible human consequence that gives the techno-medico-legal problem its distinctive moral weight, and that this paper returns to in its concluding appeal for sustained research attention.

IV. THE INDIAN LEGAL FRAMEWORK: AN INDIVIDUAL ANALYSIS

No single statute in India governs the techno-medico-legal space as a shole. Instead, a patchwork of general and sector-specific laws applies, each drafted for a narrower purpose and each bearing only partially on the problem at hand.

A. The Information Technology Act, 2000

The Information Technology Act, 2000 remains India's foundational cyber-law statute.[12] Section 43A imposes a duty of reasonable security practices on anybody corporate handling sensitive personal data or information, a category that, under the rules framed thereunder, expressly includes physical, physiological and mental health condition and medical records.[13] Sections 66, 66C and 66D criminalise computer-related offences, identity theft and cheating by personation using computer resources, all of which are directly relevant to the theft of patient identities from hospital databases, while section 72 penalises breach of confidentiality and privacy by any person who, in pursuance of powers conferred under the Act, has secured access to electronic material. Section 66F criminalises cyber terrorism and was the provision invoked in the AIIMS matter, an indication that the Act, though two decades old, retains the doctrinal

[11]Cynthia Fernandes and Rahul Matthan, "Health Data and the Missing Regulatory Middle", 14 *NUJS Law Review* 45, 52 (2021).
[12]The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[13]The Information Technology Act, 2000, s 43A read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r 3.

flexibility to address even the most severe healthcare-sector intrusions.

B. The Digital Personal Data Protection Act, 2023

India's first cross-sectoral data protection law defines personal data broadly and imposes obligations of purpose limitation, data minimisation and security safeguards on every Data Fiduciary, a category that includes hospitals, telemedicine platforms and health-tech applications.[14] Significantly, however, the Act departs from the approach of the 2011 Rules that preceded it as it does not create a distinct, heightened category of sensitive personal data for health information, choosing instead a uniform standard of protection for all personal data.[15] additionally this act also resulted on the DISHA bill not being passed, stating that a common data privacy provision will suffice all sectors. This paper argues that this is one of the most consequential legislative choices affecting the techno-medico-legal space, because it treats a patient's diagnosis with the same baseline protection as, a customer's shopping preference which is farcical.

C. Professional Medical Regulation: The National Medical Commission Act, 2019 and the Telemedicine Practice Guidelines, 2020

The National Medical Commission Act, 2019 empowers the Commission's Ethics and Medical Registration Board to regulate professional conduct, including conduct relating to the use of technology in the practice of medicine. Acting under this authority, the Telemedicine Practice Guidelines, 2020 categorise teleconsultations by mode of communication and urgency, and restrict the classes of medicine that may be prescribed remotely, dividing drugs into List O, freely prescribable, List A, prescribable only after a first physical consultation, and List B, prescribable in follow-up teleconsultations.[16]

These Guidelines are a rare example of a genuinely techno-medico-legal instrument, drafted jointly with technology and medicine in view, yet they remain subordinate legislation, issued as an appendix to an ethics regulation, and carry none of the enforceability, funding or

[14]The Digital Personal Data Protection Act, 2023, s 8 (obligations of Data Fiduciaries) and s 9 (processing of children's data).
[15]The Digital Personal Data Protection Act, 2023, s 2(t) read with s 4; the Act does not, unlike the erstwhile 2011 Rules, carve out a distinct heightened category for health data, a lacuna discussed in Part V of this paper.
[16]Telemedicine Practice Guidelines, 2020, cl 3.1-3.6 (categorisation of teleconsultation and prescribing limits).

institutional weight of a standalone statute.[17]

D. The Drugs and Cosmetics Act, 1940 and the Regulation of E-Pharmacies

The sale of medicines through online platforms, an activity that grew explosively alongside telemedicine, is regulated, imperfectly, through the Drugs and Cosmetics Act, 1940 and the Rules framed thereunder.[18] Dedicated E-Pharmacy Rules have been drafted and re-drafted over successive years but remain unenforced, leaving online pharmacies to operate under the same licensing framework designed for brick-and-mortar chemists, a framework ill-suited to questions of data retention, algorithmic recommendation of medicines, and cross-border fulfilment.

E. The Health Data Management Policy and Ayushman Bharat Digital Mission

A draft Digital Information Security in Healthcare Act was proposed as early as 2018 to create a dedicated health-data regulator with the power to enforce a patient's ownership and control over their own medical records, but it was never enacted.[19] Its conceptual legacy survives in the Health Data Management Policy notified under the Ayushman Bharat Digital Mission, which establishes a consent-based architecture for the collection, storage and sharing of health records across the federated digital health ecosystem.[20] This Policy, however, is an executive instrument issued by the National Health Authority and does not carry the force of a parliamentary statute, meaning that its consent safeguards are enforceable, at best, through the general provisions of the Digital Personal Data Protection Act rather than through any healthcare-specific remedy.

F. The Clinical Establishments Act, 2010

At the institutional level, the Clinical Establishments (Registration and Regulation) Act, 2010 requires registered establishments to maintain and provide records and reports as prescribed, a provision that has increasingly been read to encompass electronic health records, but the Act was drafted with paper registers, not networked databases, in contemplation, and

[17]Telemedicine Practice Guidelines, 2020, cl 5.1 (List O, List A and List B medicines).
[18]The Drugs and Cosmetics Act, 1940, No. 23, Acts of Parliament, 1940 (India), read with the Drugs and Cosmetics Rules, 1945, r 65(11A) (e-pharmacy) inserted by the (yet to be finally notified) E-Pharmacy Rules.
[19]Ministry of Health and Family Welfare, *Draft Digital Information Security in Healthcare Act (DISHA)* (2018) (never enacted, but influential in shaping the Health Data Management Policy).
[20]National Health Authority, *Health Data Management Policy* (2022), Ayushman Bharat Digital Mission, paras 5-9 (consent architecture and purpose limitation).

says nothing about cybersecurity standards, breach notification, or the interoperability that the Ayushman Bharat Digital Mission now demands.

G. Criminal Law, CERT-In Directions and Consumer Protection

The Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, 1860, retains and at times sharpens offences relevant though not in name, but which can be applied to healthcare fraud, including forgery and cheating by personation, offences with obvious application to the theft or manipulation of digital medical identities.[21] Separately, the mandatory breach-reporting Directions issued by the Indian Computer Emergency Response Team in April 2022 require any body corporate, including hospitals, to report cybersecurity incidents within six hours of detection, a stringent timeline that, if properly enforced, could have accelerated the institutional response to the AIIMS breach.[22] Finally, the Consumer Protection Act, 2019 has been read by courts and commentators to extend consumer remedies to services rendered through telemedicine platforms, giving patients a further, if indirect, avenue of redress against negligent or fraudulent digital healthcare providers.[23][24]

V. THE TECHNO-MEDICO-LEGAL INTERSECTION

The Indian legal framework does not lack provisions relevant to telemedicine, e-health and healthcare cybersecurity, it only lacks a coherent architecture that connects them. Each statute was drafted from within a single discipline, information technology law, medical ethics, or consumer protection, and each therefore addresses only one facet of the triangular problem.[25] For example, when a ransomware attack takes place on a hospital's electronic health record system, the Information Technology Act supplies the criminal offence and the breach-reporting obligation, the Digital Personal Data Protection Act supplies the data-fiduciary's civil liability to the patients whose data was compromised, the Telemedicine Practice Guidelines and the National Medical Commission Act govern whether the treating doctor can be held

[21]The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India), ss 111, 303, 336-338 (offences relating to forgery and cheating by personation, applicable to identity-based medical fraud).
[22]The Indian Computer Emergency Response Team (CERT-In) Directions of 28 April 2022 issued under s 70B(6) of the Information Technology Act, 2000, cl (ii)-(iv) (six-hour breach reporting mandate).
[23]The Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India), s 2(42) (definition of "service", extended by judicial interpretation to teleconsultation).
[24]Indian Medical Association v Union of India, (2019) SCC OnLine Del, discussing the applicability of the Consumer Protection Act to medical services rendered through digital platforms.
[25]Rahul Matthan, "The Triangular Problem: Why Health-Tech Regulation Cannot Be Left to a Single Ministry", 5 *Indian Journal of Law and Technology* 88, 91-94 (2022).

professionally accountable for continuing to prescribe medicine through a compromised, unencrypted channel and the Clinical Establishments Act determines whether the hospital itself can be deregistered for failing to maintain adequate records. No single regulator, and no single court of first instance, is equipped to adjudicate all four dimensions of the same factual event.[26]

The constitutional backdrop to this fragmented landscape is the Supreme Court's recognition, in Justice K.S. Puttaswamy, of informational privacy, including medical privacy, as an intrinsic facet of the right to life and personal liberty under Article 21.[27] That recognition sits uneasily beside the earlier ruling in X v Hospital Z, which permitted disclosure of a patient's medical condition where public interest so required, illustrating that even within the judiciary the balance between medical confidentiality and competing interests has never been settled with the precision that a digital healthcare system now demands.[28]

Compounding the difficulty, the Digital Personal Data Protection Act empowers the Central Government to exempt any instrumentality of the State, including government hospitals, from the Act's obligations, a provision that, if invoked, would leave the very institutions most likely to hold the largest troves of sensitive health data outside the reach of the country's principal data protection statute.[29] It is precisely this kind of seam, invisible to a lawyer trained only in constitutional law, a technologist trained only in systems security, or a physician trained only in clinical ethics, that interdisciplinary techno-medico-legal scholarship exists to identify.[30]

VI. A COMPARATIVE LEGAL STUDY: INDIA, THE UNITED STATES AND THE UNITED KINGDOM

A comparative glance at more mature jurisdictions throws the Indian gap into sharper relief, while also establishing caution. The United States has regulated health information privacy and security through a dedicated sectoral statute namely the Health Insurance

[26]Vikram Raghavan, *Communications Law in India* (LexisNexis, 2007) 412-415, on the difficulty of applying a single statute to converged technologies.
[27]Justice K.S. Puttaswamy (Retd) v Union of India, (2017) 10 SCC 1, paras 3(K), 638-645 (recognising informational privacy, including medical data, as intrinsic to Article 21 of the Constitution).
[28]X v Hospital Z, (1998) 8 SCC 296, paras 26-29 (limits of medical confidentiality where public interest so demands).
[29]The Digital Personal Data Protection Act, 2023, s 17(2)(a) read with s 17(4), which permits the Central Government to exempt any instrumentality of the State from the Act's obligations, a provision of particular concern for government-run hospitals such as AIIMS.
[30]Shamnad Basheer and Prashant Reddy, "Regulating Health-Tech at the Seams", 3 *NLS Business Law Review* 1, 6 (2020).

Portability and Accountability Act, 1996 (HIPAA). It establishes a Privacy Rule and a Security Rule that apply specifically to covered entities, including hospitals, insurers and, by extension, telehealth platforms that handle protected health information.[31]

The Health Information Technology for Economic and Clinical Health Act of 2009 strengthened this framework considerably, introducing meaningful financial incentives for the adoption of electronic health records alongside a mandatory breach-notification regime requiring covered entities to notify affected individuals, the federal Department of Health and Human Services, and in significant cases the media, within sixty days of discovering a breach.[32] The American model treats health data as categorically distinct from ordinary personal data, an approach India's Digital Personal Data Protection Act noticeably declines to adopt.[33] Telemedicine licensure in the United States, however, remains fragmented across state lines, and interstate practice depends on voluntary reciprocity compacts among state medical boards, a decentralisation that offers India a cautionary lesson in the costs of leaving licensure entirely to state commissions.[34]

The United Kingdom offers a different comparative lesson, one rooted in the integration of data protection law with a unified public healthcare provider. Health data is treated as a special category of personal data under the retained UK General Data Protection Regulation, read with the Data Protection Act, 2018, attracting a higher threshold for lawful processing than ordinary personal data.[35] Because the National Health Service is the dominant provider of healthcare in the United Kingdom, NHS Digital has been able to issue binding, system-wide standards, including the Data Security and Protection Toolkit, with which every organisation handling NHS patient data, including private telehealth contractors, must demonstrate compliance as a condition of doing business with the health service.[36]

Separately, the Network and Information Systems Regulations, 2018 impose mandatory

[31]Health Insurance Portability and Accountability Act of 1996, Pub L No 104-191, 110 Stat 1936 (US), codified in relevant part at 42 USC §1320d et seq.
[32]Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub L No 111-5, 123 Stat 226 (2009) (US), title XIII, subtitle D.
[33]45 CFR §§160, 164 (US) (HIPAA Privacy and Security Rules, including the Breach Notification Rule requiring notice within 60 days).
[34]Federation of State Medical Boards, *Telehealth Policy Tracker* (2023), documenting state-level licensure reciprocity compacts for interstate telemedicine in the United States.
[35]Data Protection Act, 2018 (UK), c 12, read with the retained Regulation (EU) 2016/679 (UK GDPR), art 9 (special category data, including health data).
[36]National Health Service (NHS) England, *Data Security and Protection Toolkit* (2023); NHS Digital, *Standard Contractual Requirements for Telehealth Providers* (2022).

incident-reporting obligations on operators of essential services, a category that includes NHS trusts, enforced by the Information Commissioner's Office with the power to levy substantial penalties.[37] India's fragmented public-private healthcare landscape makes the wholesale import of a single-payer regulatory lever of this kind difficult, but the underlying principle, that health data deserves a distinct legal category enforced by a body with healthcare-specific expertise, translates directly to the Indian context regardless of the underlying delivery model.

VII. SUGGESTIONS AND THE WAY FORWARD

The Justice B.N. Srikrishna Committee, whose 2018 report laid the groundwork for what eventually became the Digital Personal Data Protection Act, had itself recommended a sectoral approach to categories of sensitive personal data such as health information, a recommendation that was ultimately not carried into the final legislation.[38] This paper revives that recommendation and situates it within four concrete proposals. First, Parliament should consider a dedicated Health Data Protection Act, or, at minimum, amend the Digital Personal Data Protection Act to reinstate a distinct, heightened category for health data, carrying stricter consent, breach-notification and cross-border transfer requirements than apply to personal data generally.[39]

Second, the exemption available to State instrumentalities under section 17 of the Digital Personal Data Protection Act should be narrowed so that it cannot be invoked to shield government hospitals and telemedicine platforms from baseline security and breach-notification obligations as a public hospital's data is no less sensitive for being held by the State.

Third, the Telemedicine Practice Guidelines and the Health Data Management Policy, both currently executive instruments of subordinate or policy status, should be elevated into statutory rules with clear enforcement mechanisms and dedicated funding for cybersecurity audits of public healthcare infrastructure, as India's critical infrastructure, healthcare included,

[37]Network and Information Systems Regulations 2018 (UK), SI 2018/506, reg 11 (mandatory incident reporting by operators of essential services, including NHS trusts), enforced by the Information Commissioner's Office.
[38]Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Committee Report, 2018), recommending a sectoral approach to sensitive personal data such as health information, a recommendation not carried into the final Act.
[39]Sreenivasan Ramamurthy, "Why India Needs a Dedicated Health Data Authority", 12 *Indian Journal of Law and Technology* 233, 250-252 (2023).

remains chronically under-resourced against the scale of the cyber threat it faces.[40]

Fourth, and institutionally, India would benefit from a dedicated inter-ministerial or statutory coordination body, bringing together the Ministry of Health and Family Welfare, the Ministry of Electronics and Information Technology, and the National Medical Commission, so that future technology-driven healthcare reforms are drafted with legal and clinical expertise in the room from the outset, rather than through the retrofitting exercise that has characterised Indian techno-medico-legal regulation to date.

VIII. THE IMPERATIVE FOR FURTHER RESEARCH

It would be a mistake to treat the arguments made in this paper as a purely technical exercise in statutory cross-referencing. Behind every provision discussed above is a patient, often one with no lawyer, no technologist, and no advocate beyond the physician she trusts, who has entrusted their most intimate information, diagnosis, fertility history, mental health records etc, to a digital system they did not design and cannot audit. When that system fails, as it failed at AIIMS in November 2022, the harm is not an abstraction measured in compromised records. it is a mother unable to retrieve her child's vaccination history, a cancer patient whose treatment file has vanished into a criminal's ransom demand, a rural clinic reduced overnight to pen and paper because the digital promise that was meant to serve it instead became its point of failure.

India stands at a genuine inflection point. The Ayushman Bharat Digital Mission aspires, to bring the benefits of digital health to the remotest corners of the country. But an aspiration built on an unstable legal foundation is a promise the nation cannot safely keep. Amartya Sen observed that health achievement is inseparable from the equity of the systems that deliver it, a proposition that applies with equal force to the legal systems that protect those systems from collapse.[41] The cost of inaction is not measured in penalties or in headlines, it is measured in the quiet erosion of trust between a billion citizens and the digital healthcare system their government has asked them to believe in.

[40]Parliamentary Standing Committee on Communications and Information Technology, *Report on Cyber Security and Rising Threats* (Rajya Sabha, 2023) 34.
[41]Amartya Sen, "Health Achievement and Equity: External and Internal Perspectives", in Anand, Peter and Sen (eds), *Public Health, Ethics, and Equity* (Oxford University Press, 2004) 263, 267.

IX. CONCLUSION

Law, technology and medicine are no longer separable strands of Indian public life. They form a single techno-medico-legal triad, which needs the interdisciplinary cooperation nd regulation to strengthen the entire triangle and safeguard the patients at its centre.

Legal scholarship has, historically, been slow to follow technology, and medicine has, historically, been left to absorb the consequences of that delay. This paper is, in the end, a plea as much as it is an analysis, that Indian legal academia, the medical profession and the technology policy community invest, urgently and collaboratively, in techno-medico-legal research, so that the next cyber-attack on a healthcare system is prevented in a courtroom of ideas long before it is ever discovered in a hospital server room. The future of e-heath and telemedicine in India, and with it the health of the nation, depends on whether the law is permitted to catch up before the next crisis arrives, or whether, once again, it is left to arrive after.