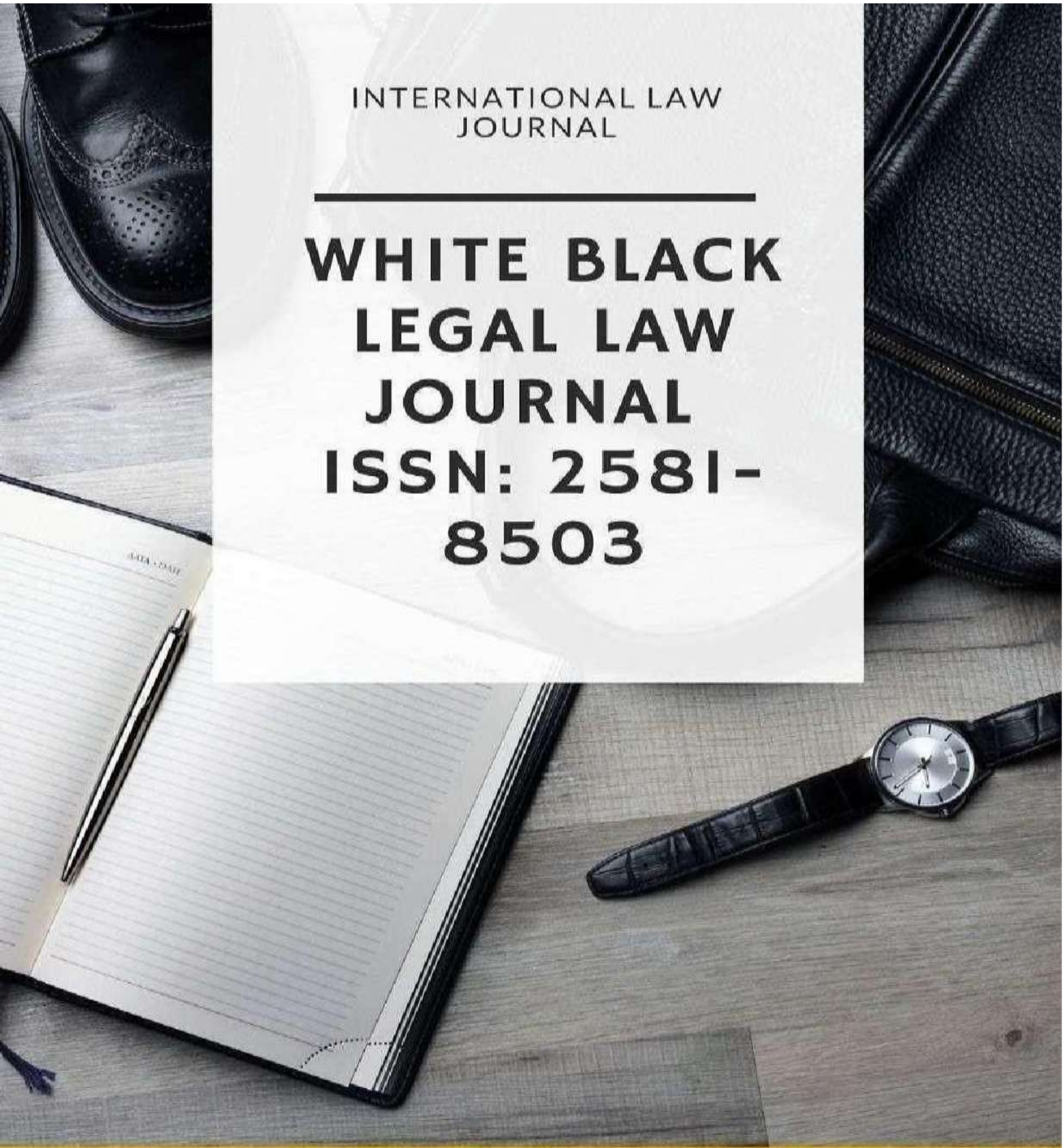

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL ISSN: 2581-8503

Peer – Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

IOT-ENABLED HEALTHCARE UNDER INDIA'S DPDP ACT, 2023: PRIVACY GAPS IN REAL-TIME DATA SYSTEMS

AUTHORED BY - GUNGUN AGARWAL & STUTI SINGHANIA

1. Introduction:

India's healthcare system faced a crimpling hit to its cybersecurity defences. In November 2022, the premier healthcare institution, All India Medical Sciences (AIIMS) hit by a ransomware attack and its operations were paralysed for 12 days.[1] The attackers targeted networked medical systems, including patient monitoring devices, forcing physicians to use manual records while patient data was extracted.[2]

This incident exposed the fragility of India's healthcare system's digitalisation. This risk has increased as Internet of Things (IoT) technologies have integrated into the healthcare industry. These days, wearable technology, smart infusion pumps, continuous glucose monitoring, and remote diagnostic tools all produce streams of real-time health data. Over 500 million records will be connected via the Ayushman Bharat Digital Mission's national digital health ecosystem, and by 2025, the wearable health device market is expected to reach $2 billion. While these advancements promise better medical delivery, they also need a great deal of data sharing between hospitals, device makers, cloud providers, and analytics firms.

In justice K.S. Puttaswamy v. Union of India, the Supreme Court upheld the fundamental right to privacy, with a specific emphasis on safeguarding private medical data.[3] As patient data moves beyond traditional doctor-patient relationships to numerous commercial entities, frequently without sufficient patient understanding or control, IoT healthcare systems pose a threat to this protection.

[1] *AIIMS Delhi: Held to Ransom by Cyber Attack*, ***NEW INDIAN EXPRESS*** *(Nov. 28, 2022), https://www.newindianexpress.com/cities/delhi/2022/Nov/28/aiims-delhi-held-to-ransomby-cyber-attack-2522960.html*

[2] Cyber Media Alliance, *AIIMS Ransomware Attack* (Feb. 2, 2026), https://www.cm-alliance.com/cybersecurity-blog/aiims-ransomware-attack

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

In response, India created the Digital Personal Data Protection Act of 2023 and the Digital Personal Data Protection Rules of 2025, which set forth standards for fiduciary accountability, data security, consent, and breach notification.[4] Although these measures reflect legislative progress, they are more of a broad framework than sector-specific legislation.

The governance issues of continuous, multi-entity IoT healthcare systems are examined in this paper, with a focus on cross-border data transfer, accountability across intricate data chains, and static consent methods.

2. IoT- Enabled Healthcare and Privacy Risks

Electronic medical records and IoT healthcare systems operate entirely differently. Documents such as blood test results or a doctor's remark from a single visit are captured in paper files or electronic medical records (EMRs). IoT devices are permanent. A continuous glucose monitor continuously measures blood sugar levels every five minutes. Every day, a single patient produces 288 readings. This adds up to thousands of data points over the course of a month, revealing not only diabetes control but also patterns of stress from everyday activities, exercise habits, and diet plans. Wearable cardiac devices continuously monitor heart rhythms. Every puff is timestamped by smart inhalers. The motions and breathing patterns of patients are sensed by hospital beds. There have never been privacy issues with a paper system because of this ongoing data collection. [5]

When computers integrate all this knowledge, the greatest risk arises from what they can deduce. A fitness tracer logs 8,000 steps in addition to GPS location information. Insurance firms can only see you when you walk on the weekends and in the evenings. They assume that your desk job is stressful. Every workday, around 3 PM, health rate spikes indicate work-related stress. Three evenings a week of insufficient sleep suggests anxiousness. All of this is not included in your medical records, but businesses create through lifestyle profiles for employment screening or insurance pricing. It is never consented to by the patients. Data, they believe, remains their physician. In actuality, these patterns are purchased by advertising and insurance without being asked.[6]

[4] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

[5] M. Abdulmalek et al., *IoT-Based Healthcare Monitoring Systems: A Survey*, 10 HEALTHCARE 1993, 1996 (2022).

[6] M. Sarrab & F. Alshohoumi, *Privacy Concerns in IoT-Based Healthcare Systems*, 11 Int'l J. Computing & Digital Sys. 123, 129 (2020).

Before your doctor sees it, every piece of health information goes via five different companies. The hardware is first constructed using proprietary software by the device manufacturer, such as Fitbit. After processing the raw data, a mobile app generates notifications. Global servers are used by third-largest cloud companies to store encrypted data streams. Fourth, specialized analytics companies use artificial intelligence models to identify trends in disease. Fifth, summary reports are sent to drug companies, researchers, or insurance. Every link functions in accordance with distinct legal and security requirements. When hackers attack, there is disagreement over who should protect the data. One responsible party is required by data protection legislation. IoT assigns culpability to five continents.[7]

In this system, consent totally fails. Over 86,000 distinct data points are produced every day by a single wearable that tracks temperature, GPS, sleep, steps, and heart rate. For 86,000 things, no one can grant explicit permission. When they purchase the gadget or enter the hospital, patients sign a single general form. Their breathing patterns are never discovered by California servers or insurers, who use sleep data to analyze their weekend drinking activities. Consent fatigue results from this. People do not click "accept" because they are aware of the risks; they do so only to get therapy.[8]

Medical equipment does not include an escape button. You run the danger of diabetic coma if you turn off your insulin pump. Arrest the heart by disconnecting the implant. Turn off the NICU's neonatal monitor to prevent early detection of respiratory issues. IoT in the medical field links privacy to survival itself, unlike shopping apps that allow you to remove your account. Not sharing data is the same as not receiving life-saving treatment. As part of their treatment, patients relinquish the power. [9]

Continuous data gathering, unseen profiling by strangers, accountability divided across five businesses, unfeasible consent standards, and an inability to disconnect safely. Regular data protection laws deal with individual companies and one-time forms. New regulations for digital hospitals are required by IoT healthcare.

[7] L. Lederman et al., *The Role of IoT in Healthcare*, 12 Health Pol'y & Tech. 45, 52 (2021).
[8] A. Sood et al., *Challenges in Digital Data Protection in Indian Healthcare*, 8 npj Digital Med. 12, 15 (2025).
[9] *Data-Protection-in-IoTEnabled-Healthcare-Ensuring-Safety-in-the-Digital-Era.docx,* § 5.4

3 Data Breaches and Case Studies

Data breaches put data protection regulations to the test under actual pressure. One malfunction in IoT healthcare, where devices continuously transmit patient data over networks, can be disastrous. Monitors connected cease to function. Medical records are sold by hackers. Digital care loses patients' trust. During disruptions, paper records are managed by regular hospitals. Complete blindness occurs in IoT hospitals. The following examples demonstrate how connectivity may transform useful tools into security headaches.

3.1 The SingHealth Data Breach, Singapore (2018)

Singapore's healthcare system is among the best in Asia. In July 2018, they also had a spectacular failure. Four million people are served by SingHealth, a nationwide hospital company that was breached by hackers. Attackers took 1.5 million patients' personal information. This contained full medication histories, phone numbers, addresses, national ID numbers, and names. No one is safe, as evidenced by the release of Prime Minister Lee Hsien Loong's diabetic treatment data.[10]

Everything was easy at first. One physician's laptop was attacked with malware. Sections of hospital networks were not separated by barriers. Hackers sprang to file servers from the laptop. Databases for patients come next. Next, to linked medical devices. Attackers were allowed to wander for three weeks. Unusual traffic was overlooked. No alarms went off. Networks were built by SingHealth for quick access to doctors, not for hacker protection.[11]

Basic errors were discovered during the research. Physicians used "password123." The software used by medical systems came out in 2014. Office PCs and patient care devices were not separated by any networks. Accounting spreadsheets shared paths with connected lab equipment and X-ray devices. Everything was destroyed by a single weak link.[12]

Singapore was quick to react. SingHealth was hit with a record-breaking S$1 million fine by

[10] SingHealth, *Joint Press Release by MCI and MOH: SingHealth's IT System Target of Cyberattack* (July 20, 2018), https://www.singhealth.com.sg/news/announcements/joint-press-release-by-mci-and-moh-singhealths-it-system-target-of-cyberattack

[11] *Personal Info of 1.5m SingHealth Patients Stolen*, STRAITS TIMES (July 20, 2018), https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

[12] Committee of Inquiry, *Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services* 45–52 (2019).

its data protection authorities. They constructed a Health Sector Cybersecurity Operations Center, which is more significant. Every public hospital is monitored by these personnel around-the-clock. They came up with stringent separation guidelines. Today, patient monitors operate on separate networks. Physicians have separate office connections. Devices are tested on a monthly basis by all hospitals. Every quarter, staff members receive training on phishing attempts.[13]

The attack was probably sponsored by China. They sought the medicinal secrets of Singapore. Even sophisticated systems fail if they are not continuously monitored. Although it doubles targets, connectivity aids in treatment. Millions were spent by Singapore to repair what appeared to be indestructible.

3.2 Indian Healthcare Breaches: AIIMS Delhi and Emerging Trends

India has less money and more challenges. AIIMS Delhi experienced a ransomware nightmare in November 2022. The premier government hospital in India fell entirely offline. Registration of patients was halted. Lab reports disappeared. Orders were written by doctors on paper. Signals were lost on live cardiac monitoring.

Test results took hours to arrive in emergency rooms. The outage continued for twelve days.[14] A total of 1.6 gigabytes of data were stolen. Among these were real-time inputs from patient monitoring devices. Dark web markets sell medical history. The assailants wanted ransom. Payment was denied by AIIMS. The patients suffered the most. Serious cases were transferred to private hospitals. Rescheduled tests took weeks for patients in rural areas.[15]

The precise point of entry is unknown. probably manufacturer laptops or servers without patches. Public hospitals without security budgets rush digital upgrades. Everything from staff Facebook to patient records is served by a single internet line. Equipment is fixed by outside businesses without conducting background checks. Vendor networks are not audited.[16]

The pattern is supported by government statistics. The number of healthcare cyberattacks

[13] Ministry of Health Singapore, *Health Sector Cybersecurity Operations Centre Launch* (2020), https://www.synapxe.sg/media-releases/cybersecurity/

[14] *New Indian Express*, "AIIMS Delhi: Held to Ransom by Cyber Attack" (28 Nov 2022).

[15] Cyber Media Alliance, "AIIMS Ransomware Attack" (2 Feb 2026).

[16] *Data-Protection-in-IoTEnabled-Healthcare-Ensuring-Safety-in-the-Digital-Era.docx*, § 5.1.

increased by 30% between 2024 and 2025. Sixty-seven percent began with non-hospital organizations. Errors in cloud storage caused the most harm. Databases were made public by vendors. Default passwords were used by security cameras.[17] Updates were absent from low-cost software. Eight patients suffer three losses. First, sudden disruptions in treatment are fatal. Cancer scans take longer than expected. Dialysis equipment malfunctions. The second is the explosion of identity theft. Perfect fraud profiles are produced with complete medical records. Third, people become afraid. Digital registration is rejected by patients. New systems are avoided by doctors.

3.3 Liability Ambiguity under India's DPDP Framework

There are 72-hour breach warnings under the DPDP rules.[18] They are given by whom? Hospitals identify assaults. Device manufacturers provide firmware that isn't perfect. Keys to encryption are lost by cloud providers. The stolen feeds are processed by analytics companies. Once a "data fiduciary" is chosen, the law ends. No rules of shared blame exist.[19]

American cloud companies cannot be sued by patients in Indian courts. Hospitals accuse vendors. Device manufacturers are held accountable by vendors. No one covers damages. In response to their incident, Singapore established dedicated health cyber teams. India uses a single universal data board for everything, making it unprepared for complicated medical issues.

4. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND DPDP RULES, 2025

Basic guidelines for digital personal data are established under India's Digital Personal Data Protection Act, 2023, and Rules, 2025. Every sector is treated equally under the law. No special attention is given to healthcare. Patient data is continuously generated by IoT devices for many businesses. This broad strategy leads to issues.[20]

4.1 Scope and Relevance to Healthcare IoT

All digital personal data pertaining to identifiable individuals is covered under DPDP. Monitors

[17] Nat'l Crime Records Bureau, *Crime in India 2024* ch. 17 (2025).
[18] Digital Personal Data Protection Rules, 2025, r. 18(1).
[19] Digital Personal Data Protection Act No 22 of 2023, § 2(13).
[20] Digital Personal Data Protection Act No 22 of 2023, Preamble.

and wearables are obviously eligible. Two roles are defined under the law. Patients are the data principals. Processing purposes are decided by data fiduciaries. This position is usually filled by hospitals.[21] IoT healthcare is a wonderful fit. Every day, 288 readings are sent by glucose monitors. Continuous cardiac implants flow. DPDP consent and security regulations apply to all data. But the law depicts straightforward relationships. Just one patient.

IoT is ideal for healthcare. Every day, 288 readings are sent by glucose monitors. Continuous cardiac implants flow. DPDP consent and security regulations apply to all data. But the law depicts straightforward relationships. Just one patient. Just one hospital. Device manufacturers, apps, clouds, and analytics companies are all involved in IoT. This intricate network is disregarded by single fiduciary norms.[22]

4.2 Rule 4 Consent Requirements

Free, explicit, informed, and revocable consent is required by Rule 4. Data use is explained in a clear notice.[23]

IoT reality is not met by this. Every day, thousands of readings are produced by devices. 288 times a day, no one gives their approval. At admission, patients sign once. That includes countless data transfers in the future. Revocation is not possible. If you disconnect your cardiac monitor, you could die. One-time tests work well with static consent. Constant updates are necessary for continuous streams.[24]

4.3 Security Measures and Notification of Breaches

Fiduciaries are required to implement appropriate security measures. Rule 18 mandates that patients and regulators receive 72-hour breach alerts.[25]

Silence is broken by seventy-two hours. But "reasonable security" isn't defined. Vendor access, heterogeneous networks, and defective devices are the main causes of IoT dangers. Medical gadgets are not subject to any particular norms. Before there is clarity, there are breaches.[26]

[21] *Id.* § 2(13).
[22] *Data-Protection-in-IoTEnabled-Healthcare-Ensuring-Safety-in-the-Digital-Era.docx*, § 3.2.
[23] DPDP Rules 2025, r. 4(1).
[24] *Id.* r. 4(2)(c).
[25] *Id.* r. 18(1).
[26] *Data-Protection-in-IoTEnabled-Healthcare-Ensuring-Safety-in-the-Digital-Era.docx*, § 4.3.

4.4 Important Data Custodians

Large processors are classified as substantial data fiduciaries under Rule 12. They have to hire executives and perform impact evaluations.[27] Large hospitals are easily eligible. Despite the same concerns, small clinics are exempt from rules. Thousands are served by rural centers without assessments. Everywhere, one breach means calamity.[28]

4.5 Critical Analysis

Progress is brought about by DPDP. Nothing beats the rules of consent. Patients benefit from breach alerts. Rules provide practical information.

Healthcare IoT is crippled by gaps. Data floods are ignored by static consent. Multi-company chains are missed by a single fiduciary model. There are no security requirements that apply to specific devices. Big hospitals are overworked. Small clinics are not adequately regulated. Without specific solutions, general laws cannot regulate specialized digital hospitals.

5. Implementing Data Protection in IoT Healthcare

5.1. One time Consent: A Lacuna

In the contemporary era of digital health governance one of the central weakness lies when a continuous reliance is placed on static consent in a dynamic environment where the space calls for continuous data generation. Internet-of-Things (IoT) used in medical setup by default produces persistent streams of biometric and behavioral information which usually counts as hundreds of data points per day. In such circumstances, one time authorization given doesn't amount to the meaningful consent and if granted hollows the substance of giving consent. Traditional models presumes the informational stability right at the moment consent is granted; however IoT instead functions through dynamic purposes, algorithm inference and secondary processing.

This very arrangement is described as the temporal misalignment between what is given consent for and what is it used for; individuals agree at one point of time however the data is repurposed indefinitely afterwards.[29] Informed consent which ensures autonomy there exists a

[27] DPDP Rules 2025, r. 12(1).

[28] *Data-Protection-in-IoTEnabled-Healthcare-Ensuring-Safety-in-the-Digital-Era.docx*, § 4.1.

[29] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1883–84 (2013).

doctrinal assumption; in high frequency data environment it does weakens the setup. Apart from being an assumption the empirical studies have consistently demonstrated that the users rarely read or comprehend the privacy disclosures, primarily in healthcare context in pretext to stress of urgent treatments decisions which the individuals undergo.[30]

Static Consent is substantive but poses a higher risk of becoming symbolic. The threat being the right word it does risk the authorization given by patient since the new uses of data is less like adaptable, the informational self- determination is merely reduced to a formal tick box rather than being a right. Dynamic consent dashboards- interfaces which allows individuals to modify the permission wherever and whenever have already been piloted in several digital health systems. Their existence demonstrates that technological feasibility is not a barrier however what really is; is regulatory mandate. A legal mandate is a need of the hour a continuous consent mechanism without which the adoption will remain choice and autonomy will remain theoretical.

5.2. Legal and institutional gaps

Secondly what constitutes a barrier is fragmented responsibility across multi-actor digital health ecosystems. In the current state of healthcare advancement the data typically differs from how it flows as compared to how it does in traditional setup: herein it involves number of intermediaries in between which may influence how the data is processed, stored or even transmitted. These entities can be hospitals, device manufacturers, software vendors, cloud infrastructure providers, analytical firms and telecommunications intermediaries. Yet the only person who bears the legal responsibility is often concentrated in a single designated entity.

Such designation reflects outdated governance assumptions derived from centralized databases rather than ideal distributed digital infrastructure. In networked environments, breaches really stems from a single failure; they often arise from interacting vulnerabilities across systems.[31] Therefore when the liability is assigned to only one entity, the result is obvious which makes downstream entities to invest in compliance while upstream technology providers face minimal legal exposure.

[30] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 543–45 (2008).

[31] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* 67–70 (2015).

The inefficiency arises from the absence of joint liability rules. This protects the actual source of vulnerability remain unaccountable whereas makes hospitals penalized for breaches which originates from a third party firmware or a foreign server, which supposedly is beyond the control. Comparative legal scholarship increasingly argues that responsibility should track functional influence rather than the formal designation.[32] Distributed liability models indeed reflects real technological reality alongside strengthening deterrence by ensuring that every actor exercising the control over such a data bears legal risk.

The concept of fragmented accountability creates practical barriers to remedies for patients. To prove or determine which entity actually caused harm may require technical evidence which precisely is beyond the capacity of individuals to obtain. DPDP rules which substantively provides protection becomes uncertain further making enforcement procedurally complex; mainly because of the loophole which neither clearly provides for the allocation of shared responsibility nor is mandated by the statue.

5.3. Global Comparisons: Mature Countries

An additional layer of vulnerability is casted as the cross border data processing has become a part of the larger picture. A significant proportion of the healthcare data is stored or analyzed on foreign cloud servers because of the cost efficiency and computational scale which global infrastructure provides. In addition of supporting innovation, they possess a serious threat in the form of exposing sensitive information to the jurisdictions with varying privacy protections, surveillance regimes, and enforcements standards.

What makes health data uniquely sensitive is the nature of its own; permanent, predictive and deeply personal. Even anonymised datasets can frequently be re-identified through data linkage techniques.[33] This undermines the assumption that exporting de-identified information eliminates risk. Although the immediate access to legal remedies becomes ineffective as soon as the data leaves the domestic jurisdiction. The regulators lacks extraterritorial authority, and cross- border enforcement mechanisms are often slow or uncertain.

[32] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* 143–47 (2019).

[33] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1704–05 (2010).

The main component which compounds these risk is deficiency of transparency. Precisely, in healthcare sector, patients rarely knows where medical data is stored or which entity or legal system governs it. Permissive transfer regimes that allows exports unless destinations are specifically prohibited prioritize much needed administrative convenience over the substantive protection. Cross- border governance remains structurally fragile and precisely of negligible use provided if no adequacy based assessments or sector specific safeguards are employed. In the age of digitalization trust depends not only on innovation but mainly on assurance that personal data remains protected regardless of geographic location.

6. Comparative Insights

6.1. European Regulatory Approach

The framework adopted worldwide decodes and illustrates how the structural weaknesses can be addressed through layered safeguards. Analyzing what European regulatory model incorporates, three key mechanism emerges; shared responsibility, heightened protection for sensitive data, and preventive risk assessment. When multiple entities jointly determine processing purposes, they all should share legal accountability and hence is called Joint controllership.[34] The process distributes compliance incentives across the technological chain rather than concentrating them in a single node.

The causal connection between sensitive heath related data and misuse of which results in discrimination, profiling or irreversible harm calls for special protection. Stricter processing thresholds reflects the principle that certain categories of information warrant heightened safeguards. One of the key feature which reinforces this approach is the mandatory impact assessments which requires high risk systems to mandatorily undergo ex ante evaluation before their deployment. Such compliances operationalize precautions by identifying vulnerabilities early rather than relying solely on penalties after the harm occurs.

This model illustrates a boarder regulatory insight: effective digital governance depends not only on sanctions but on documentation, auditability and demonstrate compliance. Preventive accountability reduces the systemic risk while preserving technological advancement.

[34] Orla Lynskey, *The Foundations of EU Data Protection Law* 158–62 (2015).

6.2. Singapore's Institutional Response

The valuable lessons are learnt from the major cyber incidents and the institutional responses. Following a large scale healthcare data breach, Singapore introduced structural reforms emphasizing on continuous monitoring rather than solely punitive enforcement. Authorities established a dedicated cyber security operations center tasked with real-time surveillance of healthcare networks and rapid incident detection.[35]

Additionally regulators mandated network segmentation which further made medical devices, administrative systems and public interfaces operate separately on digital layers. This architectural safeguards limits cascading failures because breach in one of the segment will not automatically spread to another or maybe entire system. The reform strongly advocates how the cyber security governance is strengthened when integrated with engineering design. In complex infrastructures, legal rules alone cannot suffice, enforceable technical innovations are equally essential.

The broader implications is institutional: digital health regulation requires specialized supervisory bodies equipped with technical expertise. Generalist regulators may lack the capacity to evaluate sophisticated vulnerabilities in interconnected medical technologies. Where infrastructures affect public health, proactive monitoring becomes a necessity rather than a policy option.

7. Policy Recommendations

7.1 Making Consent Dynamic and Informed

As healthcare gets more data-centric, the intersection of law, technology, and ethics needs to be delicately managed. The emergence of more Internet of Things (IoT) devices in clinical environments enhances opportunities for diagnosis, but further complicates the distinction between medical data, consumer data, and national data sovereignty. When healthcare systems are filled with IoT devices, like a fitness bracelet that becomes a diagnostic tool an increasingly normal occurrence, then consent must be dynamic. Thus, in India, we must consider dynamic consent frameworks in Ayushman Bharat Digital Mission (ABDM) and the National Health Authority's (NHA) data-sharing programs. This will help patients change permissions in real

[35] Singapore Ministry of Health, *Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services* 12–18 (2019).

time via mobile health apps or online dashboards and thereby have agency in the data-sharing process. By approving this consent framework locally, Indian regulators could ensure that consent is not a one-time tick-the-box option, but an ongoing discussion between physician and patient.

7.2 Privacy-by-Design in Medical IoT Devices

The DPDP Act calls for "reasonable" security safeguards, but it does not include privacy-by-design principles at the product development phase. This is particularly troublesome in Medical IoT, where security problems have emerged due to the design of the medical device. India could model an alternative taken by the EU’s Medical Device Regulation (MDR) framework. They want to incorporate various functions like cybersecurity audits and data protection into the medical device certification process. The idea is to have medical devices that require independent evaluations for security measures before they are allowed into the marketplace, which builds a safety feature toward a better security posture across the entire system. Adopting a “shared liability clause” to include “co-fiduciaries” and “processors” for data responsibility would foster standard obligation across the underlying IoT chain. The NHA could also establish a registry for each IoT-approved associate, thus creating an easier assurance of accountability and auditability.

7.3 Changes to Institutions for Enforcement and Oversight

The Data Protection Board of India, established under the DPDP Act, continues to be the primary enforcement mechanism. However, the Board does not have the necessary industry experience to govern the handling of healthcare cybersecurity. An authority such as the Ministry of Health could establish a Digital Health Data Authority (DHDA) that would be responsible for the following: monitoring compliance for IoT-based medical data processing. Conducted audits of the sector and breach investigations. Partnered with CERT-In to manage incident response in a real-time manner.

7.4 Empowering patients: A human-centric data governance architecture

The current regulatory discourse around data governance in India has aimed toward strengthening institutional accountability at the expense of empowering patients. A more human-centric approach would require that data stewardship rights, such as the right to audit, correct, and port one’s health data, be entrenched in India’s regulatory architecture. The GDPR legally mandates this through Articles 15-20 and allows for actual patient control over their health data. India could legally mandate this through an interoperable personal health record (PHR) platform under the ABDM, which provides patients the ability to know when and where their health data was accessed.

Together, these measures would create a governance architecture that strengthens patient trust without stifling digital innovation.

8. Conclusion

The use of Internet of Things (IoT) technologies in health care is one of the greatest shifts in medicine occurring today. Whether through wearables that quantify physiologic metrics or through hospital systems that support the ability to monitor patients remotely from virtually anywhere in the world, the practice of medicine has been profoundly changed. Alongside examining India's Digital Personal Data Protection Act, 2023 (DPDP), this article also suggests that privacy norms may need to engage with the local conditions in health care. The Indian framework, although well-meaning, has not taken into account the real-time and multi-actor challenges of IoT-enabled health care. This article contends that the challenge for India is not a matter of law, but of structure. The IoT healthcare system comprises networks that contain diverse actors-patients, hospitals, medical device manufacturers, cloud service providers, and government platforms, one of which can process data. Without an unequivocally structured model of accountability around any one actor, the potential for gaps in accountability will be significant. This is particularly important when data handled by "IoT" systems crosses national borders.

The comparative viewpoint underscores the necessity of an effective cross-border data governance regime. Health data might traverse borders for storage in the cloud, medical diagnosis using AI, infrastructure to support international research, and others. Policymakers should articulate adequate standards and bilateral agreements that allow for international transfers of health data sufficiently safeguarded and incentivised for medical research collaborations.

Nonetheless, technical safeguards are simply not enough. India's digital health evolution should be founded upon ethical considerations. The moral underpinnings of healthcare legislation are reflected in patient autonomy, informed consent, and the right to an explanation concerning algorithmic decisions in patient care. As artificial intelligence becomes embedded into IoT medical devices, predicting diagnoses and treatment plans, customising treatment decisions to the individual context, and even prioritising patient intervention during triage in emergencies, the absence of regulation for precise AI systems may create ethical gaps and unsafe oversights. There is a need for regulatory expertise specific to sectors. If tasked with being aware of all sectors, the proposed Data Protection Board envisioned under the DPDP Act will be overwhelmed. A more effective structure is to create supervisory cells, organised by sectors or domains, particularly in the Ministry of Health, which can monitor IoT systems, examine breaches, and work with the central board. This is akin to the multi-authority structure of the GDPR, but it's suited to the public administration system in India.

Considering the stance proposed in the article, IoT-enabled healthcare is, at once, a promised opportunity and a promised obligation. India has already made clear its policy and legislative intent through the DPDP Act. Now, India must build on its digital health governance effort through conversations with global best practices. The experience of other countries makes one thing clear: data protection is not only a matter of law, but one of societal process. If India is to ensure that the digital revolution in healthcare enhances, rather than subverts, trust between patients, practitioners and pills, it must build a privacy ecosystem that is benchmarked and transparent.