Page 2723 - 2741 **DOI:** *https://doij.org/10.10000/IJLMH.1110150*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Challenges and Potential Solutions to Ensure the Privacy and Security of LGBTQ Individuals

ARUNDHATI BANERJEE[1]

ABSTRACT

The privacy of the health data for LGBTQ+ individuals in India is a very serious concern, showing systematic gaps in the healthcare industry and societal biases. The manner in which data is collected today is strict and non-inclusive, which creates negative consequences in terms of misidentification and treatment deficiencies for LGBTQ+ patients. Although technologically efficient, digitization of health information results in increased risk of privacy breaches and unauthorised access, compounded by inadequate legal protections. The current Indian legal system of the Right to Privacy, IT Act, 2000, The Digital Personal Data Protection Act, 2023 gives only partial protection without any reference to health data of LGBTQ+ community. Transgender Persons (Protection of Rights) Act, 2019 specially addresses non-discrimination in healthcare (including insurance) for transgender, but does not apply to broader LGBTQ+ health with regard to data privacy. Challenges are associated with society estimated stigma attitudes with subsequent low help-seeking behaviour, legal gaps, errors during data collection, risks of digitalisation and lack of knowledge and training for healthcare professionals. Tackling these problems will require broad responses like enactment of new legislation that clearly defines and protects sensitive LGBTQ+ health data; adoption of sensitive data-collection methods; and beefing up data security with strong encryption and tight access controls.

Keywords*: LGBTQ+, healthcare, privacy, security, sensitive data.*

I. INTRODUCTION

Healthcare facilities are a key area of concern, particularly when it comes to how sensitive information is handled (or mishandled).[2] The way health data is collected in India's healthcare system leaves LGBTQ+ individuals in a precarious position.[3] A key problem is that data collection methods haven't kept up with the times; many places still stick to a rigid "male or female approach", turning a blind eye to the diverse realities of sexual orientation and gender

[1] Author is a Research Scholar at DBS Global University, Dehradun, India.

[2] Javad Pool and others, 'A Systematic Analysis of Failures in Protecting Personal Health Data: A Scoping Review' (Elsevier Ltd, 1 February 2024).

[3] Dia M Toi and others, 'TOP EDITORIA' <https://timesofindia.indiatimes.com/blogs/developing-contemporary-india/indias-health-systems-exclude-lgbtq-people-this-needs-to-change/>.

 [ISSN 2581-5369]

identity. This can lead to LGBTQ+ patients being misidentified or simply not seen for who they are, which can mess up their records and result in them not getting the right treatment.[4] On top of that, the fear of facing judgmental or ignorant questions from a healthcare staff can make LGBTQ+ individuals clam up about their medical history, which is like shooting themselves in the foot.[5]

Storing sensitive health data is also a major headache. While going digital with health records is supposed to make things easier, it also opens the door to data breaches and hacking.[6] Though India is making strides in data protection, the safeguards may still be a far cry from what's needed to truly protect LGBTQ+ individuals highly sensitive information.[7] It's easy to imagine a data leak or lax security at a healthcare facility exposing this data, which could lead to severe repercussions, from being shunned by society to facing discrimination and even violence, given the deep seated stigma surrounding it.[8]

Sharing LGBTQ+ individual's health data, both within and outside of healthcare settings, is another area rife with problems.[9] Within the healthcare system, the lack of clear rules and strict "need-to-know" policy can lead to sensitive information being spread around unnecessarily among healthcare workers.[10] What's more, there are serious concerns about this data potentially being shared with family members, insurance companies, or other third individuals' full and informed consent.[11] The fact that there aren't strong legal frameworks and enforcement measures to prevent this unauthorised sharing just adds fuel to the fire.

These vulnerabilities are made even worse by broader societal issues. As Rico pointed, out deep-rooted stigma and discrimination against LGBTQ+ individuals create a perfect storm for their health data to be misused, with potentially disastrous consequences. In a country where many people still struggle to accept same-sex relationships and diverse gender identities, having someone's LGBTQ+ status revealed through their health records can have catastrophic

[4] Corinna CD Franklin, 'Poorer Health in the LGBTQ+ Community Due to Fear of Mistreatment' (2023) 5 Journal of the Pediatric Orthopaedic Society of North America 625.
[5] Janice A Sabin, Rachel G Riskind and Brian A Nosek, 'Health Care Providers' Implicit and Explicit Attitudes toward Lesbian Women and Gay Men' (2015) 105 American Journal of Public Health 1831.
[6] Liu Hua Yeo and James Banfield, 'Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis', vol 19 (2022) <https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/>.
[7] 'Living with Dignity Sexual Orientation and Gender Identity-Based Human Rights Violations in Housing, Work, and Public Spaces in India' (2019).
[8] Adil Hussain Seh and others, 'Healthcare Data Breaches: Insights and Implications' (MDPI AG, 1 June 2020).
[9] Brenda L Beagan and others, 'LGBTQ+ Identity Concealment and Disclosure within the (Heteronormative) Health Professions: "Do I? Do I Not? And What Are the Potential Consequences?"' (2022) 2 SSM - Qualitative Research in Health.
[10] Peter F Edemekong and others, 'Health Insurance Portability and Accountability Act (HIPAA) Compliance Continuing Education Activity' <https://www.ncbi.nlm.nih.gov/books/NBK500019/>.
[11] 'CONCEPTS AND VALUE OF PRIVACY' <https://www.ncbi.nlm.nih.gov/books/NBK9579/>.

 [ISSN 2581-5369]

social, economic, and sometimes even legal repercussions.[12]

There's a crying need to pay closer attention to how breaches and misuse of health data can lead to deliberate discrimination and harm against queer individuals in India.[13] This is due to the systematic weaknesses in the healthcare system and the deeply ingrained prejudices in society. LGBTQ+ individuals already face discrimination in many aspects of life, including healthcare, so the exposure of their health data just adds insult to injury and could have devastating consequences.[14]

Loose data security protocols, inadequate staff training and a lack of strong digital defences leave LGBTQ+ patients health records vulnerable to unauthorised access.[15] This is especially problematic because information about sexual orientation, gender identity and specific health needs, like HIV status or gender-affirming care, is highly sensitive.[16]

The impact of these breaches can be catastrophic. Revealing someone's LGBTQ+ status without their consent can lead to them being shunned by society, abandoned by family and community, losing their job, and suffering physical or mental harm. In a society where stigma and discrimination against LGBTQ+ people are widespread, the misuse of health data can have far-reaching and long-lasting consequences, potentially pushing individuals even further to the fringes of society.[17]

Furthermore, the intersection of legal and social factors muddies the waters even more. While India has made progress in acknowledging LGBTQ+ rights, it still lacks comprehensive legal safeguards for data protection, particularly concerning sexual orientation and gender identity, which are still up in the air.[18] The concern is that without specific legal protections in place, LGBTQ+ people are left at the mercy of potential discrimination based on their health information, with little recourse if that information is misused.[19]

---

[12] 'LGBT Rights - Amnesty International'.
[13] Lakshya Arora, PM Bhujang and Muthusamy Sivakami, 'Understanding Discrimination against LGBTQIA+ Patients in Indian Hospitals Using a Human Rights Perspective: An Exploratory Qualitative Study' (2022) 29 Sexual and Reproductive Health Matters.
[14] Katelyn M Sileo and others, 'Assessing LGBTQ+ Stigma among Healthcare Professionals: An Application of the Health Stigma and Discrimination Framework in a Qualitative, Community-Based Participatory Research Study' (2022) 27 Journal of Health Psychology 2181.
[15] 'Advancing LGBTQ Equality Through Local Executive Action - Center for American Progress'.
[16] Ann-Sylvia Brooker and Hannah Loshak, 'A Service of the National Library of Medicine' <https://www.ncbi.nlm.nih.gov/books/NBK564233/>.
[17] 'Discrimination Prevents LGBTQ People From Accessing Health Care - Center for American Progress'.
[18] Gajanan Bonsale and Bharati Vidyapeeth, 'ASSESSING THE STATE OF LGBTQ+ RIGHTS AND COMMUNITY IN INDIA' <https://www.researchgate.net/publication/381888098>.
[19] Brad Sears and others, 'Documenting Discrimination Based on Sexual Orientation and Gender Identity in State Employment' (2009).

 [ISSN 2581-5369]

II. CHALLENGES

- Societal Stigma and Discrimination – The widespread stigma and prejudice against LGBTQ+ people mean they're often wary of going to the doctor or sharing important health details.[20] This reluctant can throw up roadblocks to getting the care they need and make them even more vulnerable. This stigmatization of diverse sexual orientations and gender identities in India often translates into prejudiced beliefs, discriminatory attitudes and discriminatory practices in society and its institutions.[21] These attitudes can create a hostile environment for LGBTQ+ individuals, leading to fear of judgment, rejection, and risk of being mistreated.[22] As a result, many LGBTQ+ people avoid healthcare altogether, even when they're in dire straits. If they do seek care, they may not feel comfortable opening up about their sexual orientation, gender identity or related health needs, because they're worried about discrimination or receiving substandard care.[23] This silence can jeopardize diagnosis treatment, and the overall quality of care. Additionally, the pressure to hide their true selves and the fear of negative reactions can also put them at risk of negative mental health consequences, which only adds fuel to the fire.

- Deficiencies in Legal Protection – Even though India has made some headway in recognizing LGBTQ+ rights, it still falls short when it comes to having strong laws that specifically protect their health data privacy. This legal vacuum means this data is vulnerable to misuse and exploitation. While there's been some movement towards decriminalizing same-sex relationships and acknowledging certain rights, there are still no clear-cut laws to safeguard the privacy of LGBTQ+ people's health information in India.[24] This lack of clarity means there are no firm rules on how this data should be collected, stored, used and shared. Without such a framework, this sensitive information is left open to abuse, whether intentionally or unintentionally.[25] For instance, without explicit legal protection, health data could be disclosed to family members without the individual's okay, used by insurance companies to deny coverage, or even end up in the wrong hands, where it could be used to

[20] Jacqueline Cosse, Kimberly Hudson and Meghan Romanelli, 'Medicine, Access, Spirit, and Survival: An Intersectional Look at Concepts of Health among a Diverse Sample of LGBTQ Adults' (2024) 5 SSM - Qualitative Research in Health.
[21] Nelsensius Klau Fauk and others, 'Stigma and Discrimination towards People Living with Hiv in the Context of Families, Communities, and Healthcare Settings: A Qualitative Study in Indonesia' (2021) 18 International Journal of Environmental Research and Public Health.
[22] '"Just Let Us Be"_ Discrimination Against LGBT Students in the Philippines _ HRW'.
[23] Alexandra Müller, 'Health for All? Sexual Orientation, Gender Identity, and the Implementation of the Right to Access to Health Care in South Africa', vol 18 (2016) <https://pmc.ncbi.nlm.nih.gov/articles/PMC5395001/>.
[24] Sofia Weiss Goitiandia and others, 'Beyond the Bench: LGBTQ+ Health Equity after India's "No Same-Sex Marriage" Verdict' (Elsevier Ltd, 1 November 2024).
[25] OL van Daalen, 'The Right to Encryption: Privacy as Preventing Unlawful Access' (2023) 49 Computer Law and Security Review.

discriminate against or harm LGBTQ+ individuals.[26] Furthermore, the absence of a clear legal recourse for those whose data is compromised further puts this population in a precarious position.

- Inadequate Data Collection Practices – In healthcare settings, flawed data collection practices, especially the absence of standardized and inclusive ways to gather information, can lead to LGBTQ+ patients being misclassified or completely overlooked. This not only messes up the accuracy of the data but also weakens privacy safeguards.[27] Sadly, many healthcare facilities in India still depend on outdated data collection methods that assume everyone fits into a simple "male" or "female" box, and that everyone is either heterosexual or homosexual.[28] This kind of system, with its limited choices, often leads to mis categorization and marginalization, and can even result in LGBTQ+ individuals being wiped off the map, as they don't always fit neatly into the available options.[29] For instance, intake forms that only list "male", "female" and "transgender" may force queer gender individuals to choose an identity that doesn't truly reflect who they are. Similarly, questions about sexual orientation that are limited to "heterosexual" or "homosexual" leave out in the cold those who identify as bisexual, pansexual or other sexualities. This failure to collect inclusive data results in inaccurate health records, which, in turn, prevents healthcare providers from fully understanding the unique health needs and disparities faced by LGBTQ+ individuals.[30] This lack of understanding can lead to less-than-ideal or poorly informed treatment, and can further policy making and the development of targeted interventions to address these inequalities.[31] Moreover, it's difficult to track health outcomes, monitor the prevalence of various health conditions, and assess the effectiveness of healthcare services for this population if LGBTQ+ individuals aren't correctly identified in their health records.

- Risks Inherent in Digitalization – While the increasing digitalization of health records makes things more efficient and accessible, it also opens a Pandora's Box of risks like data breaches, unauthorized access, and cyberattacks. These vulnerabilities hit marginalized and at-risk groups, such as the LGBTQ+ community, particularly hard. While this growing reliance

[26] 'COMMENTARY_ Protecting Healthcare Privacy_ Analysis of Data Protection Developments in India'.
[27] Reggie Casanova-Perez and others, 'Broken down by Bias: Healthcare Biases Experienced by BIPOC and LGBTQ+ Patients', vol 2021 (2022) <https://pmc.ncbi.nlm.nih.gov/articles/PMC8861755/>.
[28] 'An Exploratory Study of Discriminations Based on Non-Normative Genders and Sexualities'.
[29] Jaime M Grant and others, 'Injustice at Every Turn A Report of the National Transgender Discrimination Survey'.
[30] Tabea Hässler and others, 'Reimagining LGBTIQ+ Research – Acknowledging Differences across Subpopulations, Methods, and Countries' (2024) 80 Journal of Social Issues 821 <https://spssi.onlinelibrary.wiley.com/doi/10.1111/josi.12643>.
[31] Sheena Asthana and Joyce Halliday, 'Developing an Evidence Base for Policies and Interventions to Address Health Inequalities: The Analysis of "Public Health Regimes"' (September 2006) 577.

 [ISSN 2581-5369]

on Electronic Health Records (EHRs) in India offers many advantages, like better coordination, fewer medical errors, and improved healthcare efficiency, it also raises the stakes when it comes to data security and privacy.[32] EHRs contain huge amounts of sensitive personal and medical information, including details about sexual orientation, gender identity, HIV status, and other very private health conditions.[33] This concentration of data makes them a prime target for cybercriminals, who may try to exploit weaknesses in healthcare systems for financial gain or malicious purposes. A data breach can happen for many reasons, including hacking, phishing scams, malware, and even threats from within the system. Moreover, many organizations cut corners on essential security measures, like using weak passwords or failing to encrypt data, which leaves EHRs wide open to unauthorized access. However, the consequences of a data breach can be especially severe for LGBTQ+ individuals. For example, having their sexual orientation or gender identity exposed can lead to discrimination, harassment, and even violence.

- Insufficient Awareness and Training – A lack of understanding among healthcare providers about the specific health needs and data privacy concerns of LGBTQ+ individuals, combined with insufficient training on handling sensitive data, can lead to unintentional disclosure or mishandling of confidential information.[34] Many healthcare providers in India are in the dark about the unique health challenges and disparities that LGBTQ+ people face. This can result in insensitive or discriminatory treatment and a failure to provide appropriate and affirming care. In some cases, healthcare providers may harbour prejudiced views about sexual orientation or gender identity, which can negatively affect the care they provide to LGBTQ+ patients.[35] They may also be unaware of the specific health needs of this population, such as the importance of hormone therapy for transgender individuals or the increased risk of certain mental stress. Mental healthcare providers should be educated on how to properly ask for and handle sensitive data related to sexual orientation and gender identity.[36] This can lead to accidental disclosure of this information to unauthorized individuals, like family members

[32] Mohd Javaid, Abid Haleem and Ravi Pratap Singh, 'Health Informatics to Enhance the Healthcare Industry's Culture: An Extensive Analysis of Its Features, Contributions, Applications and Limitations' (2024) 1 Informatics and Health 123.
[33] Chris Grasso and others, 'Planning and Implementing Sexual Orientation and Gender Identity Data Collection in Electronic Health Records' (Oxford University Press, 1 January 2019) 66.
[34] Benjamin Idoko and others, 'Enhancing Healthcare Data Privacy and Security: A Comparative Study of Regulations and Best Practices in the US and Nigeria' (2024) 11 Magna Scientia Advanced Research and Reviews 151.
[35] Jan Kilicaslan and others, 'Healthcare Professionals' Experiences and Perceptions about LGBTIQA+1' (2024) 48 Archives of Psychiatric Nursing 85.
[36] Natalie Polizopoulos-Wilson and others, 'A Needs Assessment among Transgender Patients at an LGBTQ Service Organization in Texas' (2021) 6 Transgender Health 175.

 [ISSN 2581-5369]

or other staff. This lack of proper training can also result in mishandling of health records, which can compromise the privacy and security of LGTBQ+ patients.

III. INDIAN LEGAL SYSTEM AND ITS GAPS

India has come a long way in acknowledging LGBTQ+ rights, particularly since 2018 decriminalization of homosexuality. However, a clear legal framework that protects the health data privacy of LGBTQ+ individuals is still largely missing in action.[37] Unfortunately, there's no specific law to safeguard this population, leaving their sensitive information vulnerable to misuse and exploitation. While India doesn't yet have a law tailor-made law for LGBTQ+ health data privacy, some exiting legal tools offers partial protection. These include:

1. Right to Privacy under Indian Constitution

In Puttaswamy vs. Union of India, the Supreme Court of India delivered a landmark judgment that significantly impacted the understanding and scope of privacy rights in the country.[38] The court definitively established that the right to privacy is a fundamental right, enshrined in Article 21 of the Indian Constitution, which guarantees the right to life and personal liberty. This ruling has far-reaching implications, particularly for marginalized communities like the LGBTQ+ community and their health data privacy.

Key points of the Puttaswamy Ruling

- Privacy as a Fundamental Right: The court dismissed the argument that privacy wasn't explicitly mentioned in the Constitution as being way off base, asserting that privacy is a fundamental part of an individual's dignity and autonomy.[39] This was a key point of contention in the case the Attorney General had argued that the right to privacy isn't enforceable under the Indian Constitution. The Supreme Court fired back, stressing that fundamental rights aren't limited to those specifically listed in the Constitution.[40] The court stated that the right to life and personal liberty, guaranteed by Article 21, must be interpreted broadly to include the right to privacy. It declared that privacy is a natural right, inherent to all human beings, and essential for the full and effective exercise of other fundamental rights.[41] The court also cited international human rights law,

[37] Sofia Weiss Goitiandia and others, 'Beyond the Bench: LGBTQ+ Health Equity after India's "No Same-Sex Marriage" Verdict' (2024) <http://creativecommons.org/licenses/by/4.0/>.
[38] 'Top AI Tags Protection-of-Life-and-Lib' <https://indiankanoon.org/doc/127517806/>.
[39] 'KS Puttaswamy v. Union of India_ Landmark Case on Right to Privacy'.
[40] 'India's Supreme Court Upholds Right to Privacy as a Fundamental Right-and It's About Time' (2017) <https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time>.
[41] 'Supreme Court Holds That The Right To Privacy Is A Fundamental Right Guaranteed Under The Constitution Of India - Privacy Protection - India'.

including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, both of which affirm the right to privacy.

- Link to Article 21: The judgment further solidified the connection between privacy and Article 21, asserting that the right to life and personal liberty cannot be fully enjoyed unless privacy is protected. Article 21 of the Indian Constitution is a cornerstone of fundamental rights, stating "No person shall be deprived of his life or personal liberty except according to procedure established by law." In Puttaswamy, the Supreme Court held that this "procedure established by law" must be fair, just and reasonable, and that privacy is an essential piece of the puzzle of "life" and "personal liberty" within the meaning of Article 21.[42] Privacy is essential to human agency; it empowers each person to make independent decisions about their bodies, relationships and personal information – things that are integral to living a dignified life. Likewise, personal liberty which includes both freedom from arbitrary state actions and self-determination can never be fully realized in a world where individuals constantly live under the threat of surveillance or fear of their personal data being abused.[43] Thus, according to the Puttaswamy judgment, privacy was not an ancillary right but a key cog in the core values that Article 21 seeks to protect.
- Overruling Pervious Judgments: The Puttaswamy judgment turned the tide on the earlier Supreme Court decisions that had taken a narrow view of privacy, thus paving the way for a more expansive understanding of this right. Before Puttaswamy, the status of the right to privacy in India was a mixed bag. Some pervious verdicts had suggested that privacy wasn't a fundamental right in and of itself, or was merely tacked on to other rights. For example, in A.K. Gopalan vs. State of Madras, the Supreme Court had adopted a restrictive interpretation of Article 21, focusing mainly on protection against unlawful detention. Similarly, in Kharak Singh v. State of U.P., the court had observed that privacy was not a fundamental right under the Constitution. The Puttaswamy judgment was thus a significant departure from the past. The nine-judge bench in Puttaswamy reconsidered these earlier decisions and found that they did not reflect the correct state of the law. The ruling also stated that the Constitution is a living document that must be interpreted dynamically to respond to modern needs and societal changes.[44]

[42] 'CRITICAL ANALYSIS OF ARTICLE 21 OF THE INDIAN CONSTITUTION (RIGHT TO LIFE AND PERSONAL LIBERTY)' <www.ijcrt.org>.
[43] Pradeep K N and Nandini D Patil, 'THE INTERPLAY OF PRIVACY AND DIGNITY RIGHTS UNDER INDIAN CONSTITUTION' (2024) <www.juscorpus.com>.
[44] 'Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors_'.

In overturning the previous, narrower interpretations, the Supreme Court set a higher and more expansive standard for protecting the right to privacy in India. The Puttaswamy judgment understood the dynamic nature of privacy as a multi-faceted concept, encompassing bodily privacy, privacy of choices, informational privacy, and privacy in the realm of decision-making.

- Recognition of Informational Privacy: The court acknowledged that privacy includes informational privacy and that such personal data must be safeguarded against unauthorized access, use, and disclosure. This part of the ruling is particularly important in today's digital age, where tons of personal information are collected, stored, and processed by both state and non-state actors. The court stressed that informational privacy isn't just about protection from physical intrusion, but also from unauthorized access, use and dissemination of information. It recognized that the accumulation of personal information could create a power imbalance, putting individuals at risk to manipulation, discrimination, and other harm.[45] The ruling also stressed the need for legal mechanisms to regulate the collection, storage and processing of personal data, including ensuring users have control over their data. This recognition of informational privacy has paved the way for data protection laws in India and had far-reaching implications across sectors like healthcare, finance and technology.[46]

2. The Information Technology Act, 2000

The IT Act is India's go-to legislation for cyber law. Its main aim is to provide the legal framework to regulate electronic transactions and prevent cybercrime, but it also contains data protection provisions. The IT Act was enacted in 2000 to grant legal recognition to electronic transactions and facilitate e-commerce.[47] It was a response to the increasing demand for a legal framework to regulate online activities in India. Although it focuses on commercial transactions and cybercrime prevention, it also covers some aspects of data protection, specifically regarding sensitive personal information. The Act specifies certain cybercrimes and prescribes their punishments. It additionally empowers the government to make guidelines and regulations for its effective execution. Since its enactment, the IT Act has seen a few amendments, most notably in 2008.[48] Nevertheless, it's said to fall short in

[45] Woodrow Hartzog, Evan Selinger and Johanna Gunawan, 'Privacy Nicks: How the Law Normalizes Surveillance', vol 101 (2024).
[46] 'DATA PRIVACY AND PROTECTION IN INDIA THE LAWWAY WITH LAWYERS JOURNAL > CALL FOR PAPERS > DATA PRIVACY AND PROTECTION IN INDIA' <https://thelawwaywithlawyers.com/data-privacy-and-protection-in-india/>.
[47] 'Cybersecurity Laws and Regulations Report 2025 India'.
[48] Ibid.

 [ISSN 2581-5369]

comprehensiveness to deal with the challenges presented by the fast-evolving digital landscape.

Section 43A of the IT Act addresses a body corporate's liability for failing to protect "sensitive personal data or information", leading to wrongful loss or wrongful gain to any person. The 2008 amendment introduced Section 43A. It makes a "body corporate" responsible to pay compensation to the aggrieved person if it doesn't observe reasonable security practices and procedures and as a consequence, causes wrongful loss to that person or wrongful gain to anyone.[49] A company, firm, sole proprietor or another association of persons engaged in commercial or professional activity is a "body corporate". This section assigns responsibility to organizations for safeguarding the sensitive personal data they hold. Yet, the section applies only to "body corporate" excluding other entities that may process sensitive data. Its definition of wrongful loss and wrongful gain is given in the Bharatiya Nayay Sanhita, 2023.[50]

A list of items categorized as "sensitive personal data or information" is set out in the Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) which were issued under the IT Act.[51] The SPDI Rules further outline the landscape of protection of sensitive personal data. These set out the reasonable security practices and procedures that a body corporate must follow to protect this data.[52] These rules were introduced as an addition to Section 43A of the IT Act and provided specific guidance to organizations on managing sensitive personal information. The rules require body corporates to adopt a robust security policy involving managerial, technical, operational and physical security retention, and data transfer.[53] The SPDI Rules were a move in the right direction, however, they did draw flak for not covering every aspect of data protection.

Sensitive personal data under SPDI Rules:

- ✓ Passwords
- ✓ Financial Information such as bank account details, credit cards or debit card details or other payment instrument details

[49] 'A REVIEW OF INDIA'S EXISTING DATA PRIVACY REGIME' <https://www.argus-p.com/papers-publications/thought-paper/a-review-of-the-information-technology-reasonable-security-practices-and-procedures>.
[50] 'Business Crime Laws and Regulations Report 2025 India'.
[51] 'Data Protection Laws and Regulations Report 2024-2025 India'.
[52] Ravi Singhania, 'SPDI Rules 2011: Taking a Step towards Securing Data' <https://indiankanoon.org/doc/1199182/>.
[53] 'Data Protection Compliances for a Body Corporate in India' (2023).

- ✓ Physical, physiological, and mental health conditions
- ✓ Sexual orientation
- ✓ Medical records and history
- ✓ Biometric information

Gaps and Limitations

- ➢ The IT Act and SPDI Rules predominantly obtain as applicable to a "body corporate" meaning the requirements do not apply uniformly to all entities handling the health data, such as individual healthcare practitioners, or small clinics.
- ➢ This is with a focus of compensating for wrongful loss or gain, rather than preventing data breaches and protecting individual rights.
- ➢ LGBTQ+ people have unique needs around this topic that are not part of the broad, blanket definition of "sensitive personal data or information".
- ➢ It does not provide for express concepts of consent, purpose limitation or data minimization integral to data protection principles.

3. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 is a comprehensive legislation for digital personal data processing in India. It lays down the rights of data principals (individuals whose data is processed) and the responsibilities of data fiduciaries (entities processing data).[54]

The DPDP Act is a much stronger piece of legislation for data protection compared to the IT Act. The essential purpose of the DPDP Act was to update the data protection framework in India and rectify the flaws of the IT Act and its associated rules.[55] It takes a more holistic approach to data protection, encompassing a broader set of principles and obligations. The DPDP Act pertains to the processing of digital personal data within India and the processing of personal data outside India for profiling individual within India. The purpose of the law is to balance the rights of individuals to protect their personal data with the need for organization to process data for lawful purposes.[56]

It paves the way for penalties for non-compliance, which could incentivize better data protection practices. The DPDP Act has stringent financial penalties for violations. These punishments also include multiple punishments, and some punishments can go up to 250

[54] 'Understanding India's New Data Protection Law _ Carnegie Endowment for International Peace'.
[55] 'India' s Digital Personal Data Protection Act: Key Provisions and Business Implications' <https://www.huntonprivacyblog.com/2023/08/22/india->.
[56] 'Data Protection Laws in India' <https://www.dlapiperdataprotection.com/?t=law&c=IN>.

Crore Rupees, depending on the nature and amount the provisions of the act and adjudicate upon disputes. India, meanwhile, is expected to put more emphasis on data protection, with hefty fines and specific bodies established to enforce the data protection regime.[57] The Act also lays down the responsibilities of data fiduciaries, such as requiring them to design and implement reasonable security safeguards to protect against data breaches, to inform data principals and the Data Protection Board in the event of a data breach and to conduct data protection impact assessments for particular forms of processing.[58] It also sets out specific rights of data principals, such as the right to be informed about the collection of their data, the right to access their data, the right to correction of inaccurate data, and the right to erasure of their data under certain circumstances. The DPDP Act also covers border data transfers, wherein data can be transferred outside of India, subject to certain conditions and restrictions.[59]

Gaps and Limitation

- Despite this, the DPDP Act is still a landmark development, even if it does not separate out protections for LGBTQ+ health data.
- While the Act does not specifically classify sexual orientation and gender identity as "sensitive personal data" this could provide lower safeguards for that type of information.
- The Act provides wide-ranging exemptions for government processing od data that presents the prospect for misuse of health data.
- The law is not explicit about when data portability is offered to individuals in the health sector, potentially giving them control over their health data.

4. The Transgender Persons (Protection of Rights) Act, 2019

Under the Act, this primarily means healthcare, where no person shall face discrimination because of their gender identity. It requires that healthcare facilities not to deny services to transgender individuals or discriminate against them, either wholly or partially, because they are transgenders. The Transgender Persons (Protection of Rights) Act, 2019, is an Indian law passed by the Parliament of India, aiming to protect transgender persons from discrimination and violence. It describes a transgender person as someone whose gender does not align with

[57] 'The Digital Personal Data Protection Act, 2023 Contents'.
[58] 'Data Breach and How to Prevent It under DPDP Act'.
[59] 'Digital Personal Data Protection (DPDP) Act_ Key Highlights'.

 [ISSN 2581-5369]

the gender assigned at birth, including trans-men, trans-women, persons with intersex variations, gender-queers, and other recognized socio-cultural identities like kinnar and hijra.

Key Provisions

- ✓ Prohibition of Discrimination – The Act prohibits discrimination against transgender persons in a range of areas, such as:
  - Education
  - Employment
  - Healthcare
  - Goods, facilities, opportunities, public access or enjoyment
  - Right to movement
  - Right to rent or own property
- ✓ Right to self-perceived gender identity – The Act recognizes transgender person's right to self-perceived gender identity.
- ✓ Certificate of Identity – For a transgender person, they can file an application before the District Magistrate to obtain a certificate to identity wherein their gender will be mentioned as a transgender.
- ✓ Healthcare – The law mandates the government to take measures to ensure healthcare facilities to transgender persons including:
  - HIV surveillance centres are separate
  - Sex reassignment surgeries
  - Hormonal therapy counselling
  - Approaching the health needs of transgender persons by re-evaluating medical curriculum
  - Broad medical insurance programs
- ✓ Employment – A transgender person may not be discriminated against by any government or private body in respect of employment matters, including recruitment and promotion. Each establishment has to appoint a complaint officer to address the complaints under the Act.

 [ISSN 2581-5369]

- ✓ Education – Government funded/recognized educational institutions shall provide inclusive education, sports, and recreational facilities for transgender persons without discrimination.
- ✓ Right to Residence – Every transgender person has the right to reside and be part of a household.
- ✓ Welfare Measures – The government is to take measures for the social welfare and social inclusion of transgender persons, comfort, rehabilitation, vocational training and self-employment and transgender-sensitive schemes.
- ✓ National Council for Transgender Persons (NCT) – The Act talks about the setting up of a NCT to provide social justice and welfare measures for the transgender community.
- ✓ Offences and Penalties – The Act provides for certain offences against transgender persons such as forced or bonded labour, denial of use of public places, removal from household, physical, sexual, verbal, emotional or economic abuse, etc. The penalties for these offences depend on the specific charges.

IV. POTENTIAL SOLUTIONS

- Enactment of Dedicated Legislation – The most important intervention is the passing of a specific law that explicitly protects the privacy and security of LGBTQ individual's health data. Such legislation should:
  - ➢ Provide a clear definition of sensitive personal information, which also covers sexual orientation and gender identity.
  - ➢ Set strict rules around how data can be collected, retained and shared.
  - ➢ Specify deterrent penalties for violations and specify mechanisms for legal redress.

The enactment of a specific law is essential. Any such law should start by clearly defining sensitive personal information. This definition must explicitly include sexual orientation and gender identity, leaving no room for ambiguity. It should then legislate strict rules how this data is collected, stored and used. That is, who can access the data, under what circumstances, and for what reasons. It should also outline the necessary technical and organizational measures they must take to protect the data from unauthorized access, loss or destruction. Lastly it must provide strong deterrents for those who violate the law. Penalties should be significant enough to discourage violations. It should also have provisions that give

 [ISSN 2581-5369]

individuals the right to legal recourse if their data privacy is breached, including a process for registering complaints, conducting investigations, and providing compensation.

- Implementation of inclusive Data practices

Healthcare systems should utilize comprehensive data collection practices, such as:

- Standardized forms that allow people to self-identify their sexual orientation and gender identity
- Training staff on culturally appropriate and sensitive methods of data collection
- Implementing electronic health record systems that reflect the diverse nature of identity expression.

Healthcare providers should adopt inclusive data collection methodologies. This should include standardized forms that help patients answer questions about their sexual orientation and gender identity. The forms should be designed to be respectful and simple, avoiding unnecessary, overwhelming, or highly personal questions. Healthcare workforce training should be designed to establish cultural competency and sensitivity in data collection. This training should include subjects like:

- ✓ The importance of using affirming language
- ✓ How to ask questions about sexual orientation and gender identity in a respectful way.
- ✓ The need to maintain patient confidentiality

Healthcare providers should also have EHRs structured to include diverse gender identities and sexual orientation. In addition, these systems should permit entry of non-binary gender identities and full range of sexual orientations, and be agile enough to accommodate future shifts in terminology and understanding.

- Fortification of Data Security Measures

Data security measures need to be strong enough to prevent unauthorised access and data breaches. These measures include:

- The adoption of strong encryption protocols.
- Access to health records only on a need-to-know basis.
- Regular security audits and vulnerability assessments.

 [ISSN 2581-5369]

Data protection is essential to prevent unauthorized access of data and data breaches; therefore, proper data security measures need to be implemented to secure sensitive health information. Several important components are involved in this:

✓ Encryption: Strong encryption is key to protecting data both in transit and when stored. When data is being transmitted, it should be encrypted using Transport Layer Security (TLS) or its successor. This ensures that even if the data is intercepted, it will be unreadable to unauthorized parties. Data at rest, data stored on servers or other storage devices – must also be encrypted. This makes the data unreadable if there's physical access to the hardware, which naturally protects the data in the event of a data breach or theft of equipment.

✓ Access Control: Access to health records must be limited to those with a legitimate need to know. This "need to know" principle prevents anyone not directly involved in treating a patient – including friends, family members or any other caregiver from finding out what's in the records. A combination of technical and administrative controls should be used to implement across restrictions. Technical measures include strong passwords, multifactor authentication, and role-based access control (RBAC) systems. RBAC systems provide different levels of access based on the job responsibilities of various users. Administrative controls are policies and procedures that define how access is granted, reviewed, and revoked. Access logs should be regularly audited to verify that access controls are in place and working, and to detect any unauthorized access attempts.

✓ Security Audits and Vulnerability Assessments: While investing in secure software and systems is essential, regular security audits and vulnerability assessments are also critical to identify and address any potential weaknesses in data security systems. Security audits involve systematically evaluating an organization to check its security policies, procedures, and implementation to ensure they are being followed and are effective. Audits can be internal or conducted by external third-party auditors. Vulnerability assessments involve finding exploits in available tools or security holes in applications or systems that an attacker could use, employing both automated tools and manual methods. These assessments must be done vulnerability scans should be used to create a remediation plan, which the business must act on to eliminate any deficiencies.

- Provision of Training and Sensitization

LGBTQ inclusive language should also be available and healthcare provider trained to speak to the patient in a respectful and affirming manner. This includes:

➢ Using inclusive words and staying clear of heteronormative assumptions

- Inquiring about preferred pronouns and names
- Being sensitive to and supportive of the patient's comfort and willingness to discuss their sexual orientation or gender identity
- Establishing a safe and inclusive environment

- Promotion of awareness and empowerment

Public awareness campaigns need to be run to:

- Educate LGBTQ people about their right to privacy and how they can protect their health information.
- Encourage them to take action when their rights are violated, and seek legal remedies.
- Support open conversation and de-stigmatize LGBTQ health issues.

V. RECOMMENDATIONS

The government would do well to assemble a task force of legal scholars, healthcare practitioners, LGBTQ+ advocates, and data security experts to write thoughtful and effective legislation. By implementing and enforcing internal policies and protocols that govern the use of LGBTQ+ health data, healthcare institutions will be able to establish high standards of care that are both legally complaint and informed by best practices. Civil society organizations should play a crucial role in raising awareness, providing support services, and lobbying for the policy reforms needed to protect guidelines on LGBTQ+ health data; privacy needs to be conducted with the aim of mapping and adapting them to the socio-legal context of India.

VI. CONCLUSION

To wrap it up, handling the health information of LGBTQ+ folks in India is like walking a tightrope. Despite a few glimmers of hope, the healthcare system and the legal landscape still have gaping holes, leaving this already vulnerable group out in the cold when it comes to protection from prejudice and harm. You could say the system is stuck in its ways with old-school data collection, and the lack of specific laws for LGBTQ+ health data, coupled with the risks of going digital and ill-informed healthcare staff, creates a perfect storm. The deep-seated stigma and discrimination in the country just add fuel to the fire, making it a real uphill battle for the LGBTQ+ community, who are caught between a rock and a hard place needing healthcare but fearing their sensitive information could be ticking time bomb in the wrong hands.

 [ISSN 2581-5369]

Even though the Puttaswamy ruling threw LGBTQ+ folks a lifeline with the right to privacy, and laws like the IT Act with its SPDI Rules, the upcoming Digital Personal Data Protection Act, and the Transgender Persons Act offer a bit of a safety net, none of them really hit the nail on the head when it comes to the unique dangers LGBTQ+ individuals face with their health data. The IT Act and SPDI Rules mostly point the finger at companies and talk about paying up after something goes wrong, but they don't really scare anyone straight beforehand and don't apply across the board to all healthcare providers. The DPDP Act, for all its good intentions, doesn't put sexual orientation and gender identity in the "handle with extreme care" category, even though it should. And even though it says to keep human rights in mind, it still leaves a lot of loopholes for how information can be used. As for the Transgender Persons Act, it's more about making sure everyone gets through the door of the clinic, not so much about locking down their health records once they're inside.

To truly get a handle on these issues, we need to come at them from all angles. It's high time we put pen to paper and pass a law specifically designed to shield the privacy, security, and confidentiality of LGBTQ+ folks' health information. This law needs to spell out loud and clear that sensitive personal details include sexual orientation and gender identity. It should also draw a hard line on how this information can be gathered, kept, and shared, with serious penalties and clear paths for legal action if anyone steps out of line.

What's also a must have is a top-to-bottom overhaul of how health services collect data. We need to ditch the one-size-fits-all forms and bring in standard ones that let people be themselves when it comes to their sexual orientation and gender identity. On top of that, we need to make sure healthcare workers get proper training to handle these matters with sensitivity and respect. And finally, we need to upgrade to electronic health records that can actually keep track of the diverse ways people identify.

Locking down health data tight as a drum is also absolutely key. We're talking Fort Knox-level security with strong encryption to scramble the information giving access only to those who absolutely need it one a "need-to-know" basis, and running regular check-ups on our digital defences to plug any holes before the bad guys can sneak in and spill the beans.

So, it brings it all home, truly safeguarding the health data privacy of LGBTQ+ folks in India calls for everyone to pitch-in from changing the laws and shaking up the healthcare system to fostering a more accepting society across the board. Getting this right isn't just about bits and bytes; it's about standing up for the rights, dignity, and well-being of a community that's often been pushed to the margins. If we drop the ball on this, we're just continuing to kick them

 [ISSN 2581-5369]

when they're down, making it harder for them to get the healthcare they need and potentially wrecking their lives and livelihoods all over the country.

*****

 [ISSN 2581-5369]