The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 2 | Issue 10 | October 2024
ISSN: 2583-973X (Online)
Website: www.theacademic.in

Rights to be Forgotten: A Necessary Implication of Right to Health: India's Privacy Prospects Vis-A-Vis Europe's GDPR Policy

Jane Lalnunsiami
Gujrat National Law University
janelalnunsiami@icloud.com

ARTICLE DETAILS

Research Paper

Keywords:

Data, Right to Be Forgotten, Privacy, Right to Life, State Interest.

DOI:

10.5281/zenodo.14102575

ABSTRACT

The concepts of data, privacy, life, and governmental interest hold significant importance and reverence within the field of medical healthcare. The Indian judiciary has sought to establish the right to be forgotten as a significant aspect of medical therapy, so reinforcing the right to health within the framework of the Right to life as outlined in Article 21. Nevertheless, the lack of legislative action has rendered this undertaking ineffectual and has placed individuals seeking medical assistance in a dire predicament. While the global community is increasingly embracing the importance of implementing the right to be forgotten as a crucial aspect of healthcare, India is yet to fully adopt this approach. This article explores the Indian perspective on the application of the Right to be Forgotten as an essential complement to the healthcare system in India. The author's research in this article also explores the comparison between Europe's comprehensive efforts to safeguarding individuals' privacy through the newly established right, known as the right to be forgotten, and India's data privacy bill of 2023.

1.1 RESEARCH QUSTIONS

i. Whether Right to be forgotten has been recognized by the Indian Judiciary?
ii. Does the aspect of Right to be forgotten have implications for the Right to health?

iii. To what extent does the Personal Data Protection Bill, 2023 accommodate the "Right to be forgotten"?

iv. Whether Health Data Management Policy, 2020 include the "Right to be forgotten" and erasure?

1.2 STATEMENT OF PROBLEM

The concept of "right to be forgotten" pertains to the capacity of the individuals to restrict, unlink, erase, or rectify the dissemination of personal data on the internet that is deceptive, embarrassing, irrelevant, or outdated. The recognition of the right to be forgotten as a basic right by the Supreme Court in the Privacy verdict is based on the essential nature of data or information. However, even after several judicial decisions upholding the same, the legislative framework on the same remains clouded with ambiguity and improper implementation of the same. The Personal Data Protection Bill, 2023 includes within its ambit the right to be forgotten.

However, another important facet of this right which is seldom discussed is its implications on the right to health. The Health Data Management Policy, 2022 addresses the same to some extent but it also invites speculations regarding the binding value of the same and ambiguities.

1.3 METHODOLOGY

i. The author employs the Doctrinal Research.

ii. For the purpose of research, the author will depend upon secondary sources of data like books, statutes, laws, regulations, cases, judgements and articles discussing various websites and newspaper articles.

2. THE INTERMITTENT LEAPS TAKEN BY THE JUDICIARY

The privacy landscape has been significantly altered by the European Court of Justice, which has introduced a reengineering of privacy prospects. Notably, the concept of the Right to be Forgotten acknowledges that individuals possess the entitlement, subject to specific conditions, to request search engines to eliminate links containing personal information pertaining to them. This criterion is applicable in cases where the information being processed is found to be erroneous, insufficient, irrelevant, or excessively abundant. In a similar vein, the Indian Judiciary has upheld a comparable position. The concept of the "right to be forgotten" or "the right to be erased" pertains to an individual's

entitlement to seek the deletion of their personal information or data from internet platforms. The genesis of this entitlement can be traced back to the French legal doctrine about the 'droit à l'oubli'. This would align with the prevailing tendency observed in Western countries, wherever the principle of "Right to be forgotten" is adhered to. The "right to be forgotten" has been acknowledged by the European Union Regulation of 2016.

The recognition of this right has been affirmed by the Supreme Court of India in the privacy case. The statement asserts that acknowledging this right would simply entail allowing an individual, who no longer wishes for their data to be processed or stored, to have the ability to delete it from the system in cases where the personal data/information is no longer required, pertinent, accurate, and lacks any legitimate purpose. The exercise of this right is restricted in cases where the information or data is deemed essential for the exercise of the right to freedom of expression and information, compliance with legal obligations, the performance of a task in the public interest, public health concerns, archival purposes in the public interest, scientific or historical research purposes, statistical purposes, or the establishment, exercise, or defence of legal claims.

Further, in the case of ***Subhranshu Rout Gugul v. the State of Odisha***[1], The Orissa High Court observed the importance of the right to be forgotten of an individual and how it remains unaddressed in legislation. The court was cognizant of the fact that there was a need for the implementation of the right to be forgotten in India, which was eventually introduced in Personal Data Protection Act, 2019 and later on expanded in the Personal Data Protection Act, 2023.

The possible ramifications of the right to be forgotten in the context of medical healthcare, however, have not been determined by the legal systems worldwide.

3. UNDERSTANDING THE FUNDAMENTALS OF HEALTHCARE POLICY

The concept of the "right to be forgotten" pertains on the capacity of the individuals to restrict, remove, unlink, or rectify dissemination of personal data on the internet that is deceptive, humiliating, inconsequential or outdated. The concept of the right to be forgotten is predicated upon the fundamental aspect of data or information. In this context, it is crucial to assess the differentiation between information and data, as it could have significant ramifications for data privacy legislation. The

[1] Subhraanshu Rout Gugul v. State of Odisha, BLAPL No. 4592 (Odisha High Court 2020)

differentiation between data and information, as commonly understood, may not necessarily serve as a decisive factor in the context of data protection. Nevertheless, it remains a fundamental distinction between data and information, a distinction that is also evident in international conventions and standards. The European Union's General Data Protection Regulation (EU GDPR) and Singapore's legislation both include definitions for the concept of personal data. In contrast, Australia, Canada, and South Africa utilise the word personal "information" to refer to the same concept. The relevance of the term "data" within the European Union (EU) may be attributed to the emergence of new technologies in the 1970s, which led to the availability of easily accessible datasets. This development served as a spur for the formation of a comprehensive framework for data protection.

Consistent with this perspective, the European Union's General Data Protection Regulation (EU GDPR) does not encompass the non-automated handling of personal data that is not intended to be included in a structured set of records. The safeguarding of privacy is primarily grounded in the concept of data, which exhibits diverse definitions across different geographical boundaries.

According to the Personal Data Protection Act, 2023, the term "*data*" encompasses a *representation of information, facts, concepts, opinions, or instructions that may be effectively communicated, interpreted, or processed by either people or automated systems*[2].

Whereas, Europe's General Data Protection Regulation defines personal data as; '*personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.[3]

Upon analysing the definitions of personal data provided by the General Data Protection Regulation (GDPR) and the Personal Data Protection Act, 2023, a notable disparity arises in the inclusion of information generated through human intervention under the definition of data as outlined by the Indian Legislature. Hence, it is evident that the legislative rationale for incorporating information created by non-automated methods is to encompass the expansive healthcare industry, where information storage by automated means is currently lacking. Consequently, the Indian legislation on data protection would be applicable to both forms of data processing, encompassing both automated processes and manual

[2] Personal Data Protection Bill, 2023, s.2 (h)
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art. 4(1)

procedures. The action undertaken by the draught committee is commendable. Recently, in the case of Balu Gopalakrishnan v State of Kerala[4], Kerala High Court issued measures for protecting the data of covid positive patients in the state of Kerala, which include the duty of the state government to anonymize the data before sharing it with a third party, in this the entity being a US company.

4. JUSTICE B.N SRIKRISHNA REPORT ON DATA PRIVACY REQUIREMENTS

The initial phase of India's Data Privacy journey is marked by the introduction of the data protection framework, which was put out by the Committee of Experts led by former Supreme Court judge Shri B N Srikrishna. The Committee recognised the importance of granting data principals the necessary tools to enforce their rights with relation to the related obligations of the data fiduciaries, in order to establish a strong data protection law. The aforementioned rights are derived from the fundamental values of autonomy, self-determination, transparency, and accountability. These rights aim to empower individuals with the ability to exercise control over their personal data, a crucial factor for ensuring freedom within the digital economy[5].

The report recommended that the right to be forgotten may be adopted, with the Adjudication Wing of the DPA determining its applicability based on the five-point criteria as follows:

i. the sensitivity of the personal data sought to be restricted;
ii. the scale of disclosure or degree of accessibility sought to be restricted;
iii. the role of the data principal in public life (whether the data principal is publicly
iv. recognizable or whether they serve in public office);
v. the relevance of the personal data to the public (whether the passage of time or change in circumstances have modified such relevance for the public); and the nature of the disclosure and the activities of the data fiduciary.

The aforementioned recommendation are situated under s. 20 of the Data Protection Bill of 2019. s. 20 of the Bill confers upon an individual the entitlement to limit or impede the ongoing dissemination of their data under certain circumstances. These circumstances include: (1)when the data has fulfilled its intended purpose or is no longer required for said purpose; (2) when the data was initially disclosed with the individual's consent, which has subsequently been revoked; or (3) when the data was disclosed in

[4] Balu Gopalakrishnan v. State of kerela, WP © Temp No. 84 (Kerela High Court 24 April 2020)
[5] Committee of experts under the Chairmanship of Justice B.N Srikrishna (31 July 2017). A free and fair digital economy: Protecting privacy, empowering Indiand (p.68)

violation of the PDP Bill or any prevailing legislation. Despite being included in the committee's report and draught bill, the Indian Data Privacy bill lacks an opt-out mechanism, in contrast to the European General Data Protection Regulation (GDPR). The committee concisely recognised that in cases where disclosure has occurred with the consent of a data subject, it would be reasonable for the revocation of such consent to activate the right to erasure.[6]

It is imperative for Indian data protection legislation to incorporate a mandatory consent provision, wherein individuals are required to provide their approval to the relevant authorities. Otherwise, the outcome will lead to the improper utilisation of individuals' personal data, similar to the situation observed in the Aadhaar issue, wherein the consent of the individual has been seen to be extensively manipulated. Numerous judicial rulings have emphasised the significance of consent, particularly in relation to personal data. However, the absence of a consent provision in any statute has been shown to facilitate arbitrary actions. Even when the customer's documents are no longer at the customer's house and have been willingly delivered to a bank, it was ruled in Distt. Registrar and Collector v. Canara Bank that the documents must continue to remain confidential vis-à-vis the person. Airtel's alleged use of an Aadhaar e-KYC based SIM verification process to open payments bank accounts of its subscribers without their 'informed consent' is an example of an arbitrary use of power. This is true even if the individual has voluntarily enrolled on the Project. Consent is a necessary condition for any action on the part of the state, since the Puttaswamy verdict establishes that an individual is to have control over the dissemination of material that is personal to him and that the unauthorised use of such data shall result in an infringement of his fundamental right to privacy.

Article 7 of GDPR mentions explicitly the requirement of consent by individuals for the processing of personal data relating to him or them. It also mentions that it shall be as easy to withdraw as to give consent.[7] On the contrary The Personal Data Protection Bill, 2023 introduces the concept of legitimate uses, allowing data processing without explicit consent for certain purposes such as employment, public interest, or legal obligations. This dilutes the opt-in requirement and creates ambiguity about when consent is actually necessary. As a result, users may lose control over certain data processing activities, as they may not have the power to opt out under these broad "legitimate" categories. Moreover, the Act permits data processing for purposes deemed in the "public interest" or in compliance with the law,

[6] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians (p 76)
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art 7(3)

further weakening the user's ability to opt out. This broad interpretation could override the opt-in/opt-out mechanism, limiting the user's control over how their data is used and shared This is a major threat to India's privacy prospects in medical healthcare.

5. UNDERSTANDING THE RIGHT TO ERASURE, A COROLLARY TO THE RIGHT TO BE FORGOTTEN

One of the biggest hurdles for the health organizations will likely be the GDPR "right to be forgotten" sometimes known as the "right to erasure". One of the cornerstones of the law is to strengthen individual rights, meaning organizations must honour all patient requests to erase personal data.[8] The Srikrishna Committee did not deliberate on the right to erasure which is concomitant to the right to be forgotten. The draft Personal Data Protection Bill, 2019, has a section on the Right to be forgotten. Further, an improvement from the 2019 draft is the addition of the Right to erasure under Section 18 of the 2019 Bill.[9] Article 17 of the GDPR grants the right to erasure and states that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay with certain qualifications.[10] Furthermore, Article 2(b) of EU Directive 95/46 states that 'for this Directive:

"Processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Therefore, the law of nations infers that erasure is a quintessential aspect of personal data. This is evident from the fact that the definition of processing of personal in the EU directive incorporates the principle of erasure".

Under Section 13 of the DPDP Act, individuals have the right to request the erasure of personal data, but Section 17(4) allows for exceptions where the state or certain fiduciaries can reject such requests for reasons like national security or public interest. This creates ambiguity and limits the right to erasure, which could have significant implications for health data, especially in cases where patients want their sensitive health records erased. The Health Data Management Policy emphasizes patient consent and

[8] Davis, J. Europe's GDPR privacy law is coming: Here's what US health orgs need to know. Healthcare IT News https://www.healthcareitnews.com/news/europes-gdpr-privacy-law-coming-heres-what-us-health-orgs-need-know
[9] Personal Data Protection Bill, 2019, s. 18(1)
[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art.17

control over their data, but these provisions in DPDP could override patient rights, undermining trust in the system. The GDPR will affect almost all industries, but in health, the new regulations give every patient more control over the personal data that is being collected about them, as well as how this information is used.[11]

6. HEALTH DATA MANAGEMENT POLICY, 2020

A National Digital Health Mission ("NDHM") was announced by the Central Government under which the Ministry of Health and Family Welfare ("MOHFW") published a blueprint in late 2019 recommending the creation of a National Digital Health Ecosystem ("Ecosystem") which allows for interoperability of digital health systems at the patient, hospital, and ancillary healthcare provider level. The MOHFW in 2020 approved a Health Data Management Policy ("HDM Policy") largely based on the PDP Act to govern data in the Ecosystem.[12] The HDM Policy recognizes entities in the data processing space, and data processors similar to the PDP Act, and establishes a consent framework for processing personal data.

The HDM Policy provides for rights to individuals and provides for the creation of Health IDs for individuals, Health Practitioner IDs for medical practitioners, and Health Facility IDs for operators/owners of health facilities. It mandates data fiduciaries to abide by the basic data protection principles and establishes certain compliance requirements including security practices and impact assessments. The HDM Policy additionally takes into account assent-based sharing of data and builds up a complaint redressal method through the National Health Authority. Rules for an 'NDHM Sandbox' were likewise distributed in August 2020 to empower the brooding of new advancements in a contained climate.[13]

The HDM Policy will have a significant impact on the medical and pharmaceutical industry once implemented, as healthcare institutions will have increased compliance obligations and the telemedicine sector is set to become busier than before. However, the HDM Policy has a huge conflict with the PDP Act, which may cause contention between the HDM Policy and the PDP Act. It is in this manner

[11] Howell, D. (2018, March 29). Five ways the GDPR will change healthcare. Future Health Index https://www.futurehealthindex.com/notification?durl=https%3a%2f%2fwww.philips.com%2fa-w%2fabout%2fnews%2ffuture-health-index.html
[12] National Digital Health Mission. (2020). Health data management policy.
[13] NDHM Sandbox. (2020). Enabling framework.

muddled why the HDM Policy was independently proposed, and if there should be an occurrence of contention, which may win.

[6.1] LACK OF A COMPREHENSIVE DATA PROTECTION FRAMEWORK

A robust Personal Data Protection Act should precede the HDM Policy. The Policy constitutes a vision document, outlining the minimum standards for data privacy and protection of health data for those who consent to share the same and should be astutely aligned with the law. A standalone health data management policy without the legal support of a data protection law does not provide the necessary protection to the sensitive and private information that will be shared by citizens.

There has been a precedent for the creation of standalone data sharing policies by other ministries without the protections of the Personal Data Protection Act. For example, the Ministry of Road Transport and Highways ("MoRTH") called for the digitization and bulk sharing of data to private entities from the Vahan and Sarathi databases, which housed vehicle registration and drivers' licenses information. Without adequate privacy and security protections, there is potential for this data to be misused.[14] During the February 2020 riots in North East Delhi, for instance, there were reports that the Vahan database was used to target vehicles belonging to Muslims.[15] This led to the MoRTH doing away with this data sharing policy due to privacy concerns.

[6.2] AMBIGUITY IN RIGHT TO ERASURE OF DATA PRINCIPLES

The HDM policy states that "data principals should be given complete control and decision-making power over how personal data or sensitive personal data associated with them is collected and processed further."[16] However, the policy does not allow the data principal to delete its data unencumbered. Paragraph 14.1(b)(ii) of the HDM Policy provides for "correction and erasure ofrights of data principals" which are problematic on several grounds.[17]

Firstly, there are no specified grounds apart from one stated in the HDM Policy allowing the data principal to delete its health data available with the entities part of the Ecosystem. The only ground

[14] K.J., S. (2019). An assessment of the bulk data sharing policy of the Ministry of Road Transport and Highways. Observer Research Foundation Issue Brief No. 332
[15] Saluja, N. (2020, February 27). Transport ministry to partially conceal names of vehicle owners on Vahan database. The Economic Times. https://economictimes.indiatimes.com/news/economy/policy/transport-ministry-to-partially-conceal-names-of-vehicle-owners-on-vahan-database/articleshow/74338287.cms
[16] Health Data Management Policy, 2020, para. 8.
[17] Health Data Management Policy, 2020, para. 14.1 (b) (ii)

specified by the Policy allowing deletion of data is that "storage of personal data violates any of the data protection principles". It is problematic because: (i). This ground is restrictive and is limited to the storage of data. It does not incorporate the collection and processing of personal data of the data principal. (ii). A data principal may not always have the know-how or understanding of the principles of data protection. The Policy has made a presumption of digital literacy amongst the citizens which is erroneous.[18]

Secondly, the Policy stipulates that personal data can be blocked or restricted rather than erased in case it has been mandated by law but it has not provided any instances where this might happen. Similarly, blocking and restricting personal data, rather than erasing it, in case it is prohibited by law does not specify instances where this might happen.

Thirdly, a data principal's data may not be deleted by the third party citing that it will cause a disproportionate effect on the storage, over-writing, anonymisation or other method (s) of removal. This provision does not clarify who shall be deleting data and if such decisions of such entities will be appealable. There are also concerns that the data principal's request for data deletion might be denied citing this.

Fourthly, though the Policy does provide processing personal or sensitive personal data about a child,[19] the provision on data erasure[20] does not stipulate a provision for a minor who on attaining a majority would want to delete its health data and opt-out of the National Digital Health Ecosystem.

Lastly, "HDMP does elaborate on the rights of digital principals, such as the right to confirmation and access, and the right to correction and erasure. It does not make adequate provisions in case of disputes with data fiduciaries. The policy mentions that if these requests for information are rejected, it will give the data principal the reasons for refusal, and if the principal is dissatisfied with the outcome", "*it may require the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal*."[21]

7. RIGHT TO BE FORGOTTEN: ANALYZING FUTURE POSSIBILITIES

[18] Health Data Management Policy, 2020, para. 12
[19] Ibid.
[20] Health Data Management Policy, 2020, para. 14 (b)
[21] Health Data Management Policy, 2020, para. 14 2(d)

Healthcare, particularly eHealth or cross-border healthcare, as well as research all have a stake in protecting patients' privacy when it comes to their health information. One the one hand, EU law provides extra safeguards for what it calls "sensitive data," which includes health and genetic information. Disclosure of a patient's protected health information without their consent could have serious consequences for the patient's personal and professional life.[22] Health data refers to personal information which pertains to either the physical or mental well-being of an individual. This includes data connected to the provision of healthcare and support services, which provide insights into the person's health condition. The phrase "biometric data" refers to personal data that arises from certain technical processes associated with the physical, physiological, or behavioural characteristics of an individual. These qualities enable or validate the distinct identification of an individual, such as facial photographs or dactyloscopy data. Genetic data encompasses personal information pertaining to an individual's inherited or acquired genetic traits, providing distinct insights into their physiology or health. This data is mostly derived via the examination of a biological specimen.[23]The proposed bill on data protection delineates health data as information pertaining to the physical or mental well-being of an individual, encompassing records pertaining to their historical, current, or anticipated health status. This definition also encompasses data acquired during the process of registering for or receiving healthcare services, as well as data linking the individual to the utilisation of particular healthcare services.[24]

The Indian draft bill that had expressly acknowledges health data as a discrete form of data, whereas the General Data Protection Regulation (GDPR) provides a broader definition that encompasses additional categories such as biometric and genetic data. This observation highlights the Indian Legislature's inclination towards prioritising healthcare considerations in relation to data protection and patient privacy.

8. CONCLUSION: THE FUTURE WOES OF THE PERSONAL DATA PROTECTION ACT, 2023

One of the primary concerns is the lack of comprehensive integration between the PDP Act and the HDMP. The PDP Act, modelled after international standards such as the General Data Protection

[22] The new EU Regulation on the protection of personal data: What does it mean for patients? (2019). European Patients Forum (p. 3).
[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art. 4
[24] The Personal Data Protection Bill, 2023

Regulation of the European Union, aims to protect personal data through provisions like the right to access specified in s. 13 and the right to erasure mentioned in s. 14. Conversely, the HDMP focuses specifically on health data management but does not fully align with the principles established in the PDP Act. This disjointedness creates a fragmented regulatory environment, which can lead to ambiguities and inconsistencies in enforcement. For instance, while the PDP Act emphasizes the need for explicit consent for data processing under s. 7, the HDMP may allow broader data sharing practices in the health sector without similar safeguards. This misalignment risks leaving sensitive health data vulnerable to misuse, thereby undermining the protective intent of both legislative frameworks.

The successful implementation of the PDP Act and HDMP hinges on the capacity of regulatory bodies to enforce compliance. The Data Protection Authority of India (DPAI), established under the PDP Act, is tasked with overseeing data protection practices. However, it is essential to ensure that the DPAI is adequately resourced and equipped with skilled personnel to handle the vast and complex data ecosystem in India. Internationally, the case of *Facebook Ireland v. Maximillian Schrems*[25] serves as a pertinent example. The European Court of Justice (ECJ) ruled that the transfer of personal data from the EU to the U.S. was invalid due to concerns over U.S. surveillance practices. This case underscores the importance of robust enforcement mechanisms and the need for authorities to be proactive in safeguarding citizens' rights against data breaches.

Ambiguities in the HDMP regarding the rights of data principals pose significant risks. For instance, the right to erasure, as articulated in the PDP Act, allows individuals to request the deletion of their data under specific conditions (Section 14). However, the HDMP lacks clear guidelines on the grounds for which data can be erased, leaving room for interpretation by data fiduciaries. This ambiguity can lead to inconsistent application and potential violations of privacy rights. Moreover, the PDP Act's provisions for dispute resolution (Section 29) require further clarity. While the Act outlines the process for addressing grievances, the effectiveness of these mechanisms depends on their implementation. A lack of clarity may deter individuals from exercising their rights, fearing a protracted and complex process.

It is advisable that the HDM Policy should comprehensively enumerate all the circumstances in which the data principal may exercise their right to request the deletion of their data. Moreover, it is imperative that the data principle possesses an unequivocal entitlement to delete their health data, which has been held, processed, and acquired by the data fiduciaries. The right of the data principal should not be

[25] C-498/16

withheld on the basis of ambiguous, possibly discriminatory, and capricious grounds. Minors should be granted the opportunity to exercise their autonomy by opting out of the health identification system and the National Digital Health Ecosystem upon reaching the age of majority. It is imperative that individuals are granted the unequivocal entitlement to delete the entirety of their health-related data. The inclusion of an opt-out mechanism in the PDP Bill is necessary in order to enhance the protection of individuals' Right to be Forgotten.