SYMBIOSIS LAW SCHOOL, HYDERABAD
A Constituent of Symbiosis International (DEEMED UNIVERSITY), Pune
Re-accredited by NAAC with "A++" Grade - Awarded Category - I by UGC
CENTRE FOR SPECIALISATION IN CYBER LAW STUDIES

CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

DSCI
PROMOTING DATA PROTECTION

Implementation of the Digital Personal Data Protection Act, 2023 in the Healthcare Industry

Submitted to: CCoE DSCI Chapter Meet

on September 2023
on "Data Privacy & Data Protection: Challenges & Solutions"

AUTHORS

Ms. Annapurna Munaganti Devi

Faculty-in-Charge

CSCLS-SLSH

Gayathri Viswan

President

CSCLS-SLSH

Varsha Khowala

Vice President

CSCLS-SLSH

Bevan Avil Pinto

Head of Research

CSCLS-SLSH

Kaviya Swaminathan

Co-Head of Research

CSCLS-SLSH

Varun Sanjay Baliga

Co-Head of Organizing

CSCLS-SLSH

Kanishk Shah

Member of Research

CSCLS-SLSH

Arka Chakraborti

Member of Research

CSCLS-SLSH

APPROVED BY

Dr. Santosh Aghav

Director

Symbiosis Law School, Hyderabad

ABOUT US

ABOUT SYMBIOSIS LAW SCHOOL, HYDERABAD

The idea of 'Symbiosis' is nurtured by Dr. S. B. Mujumdar on the principles of vedic thought 'Vasudhaiva Kutumbakam' which means 'World as One Family'. Symbiosis Law School (SLS) Hyderabad is established in 2014 inheriting splendid novelty, dynamism and excellence in education of Symbiosis International University, Pune. The Legacy of Symbiosis Law Schools in excellence and quality began with Symbiosis Law School Pune, which is consistently ranked among top 10 law schools in India in last 13 years.

Symbiosis Law School, Hyderabad (SLS-H) was established in the year 2014 and has now successfully blossomed into one of the premier law schools. It has been catering to the higher education of diverse group of students inheriting splendid novelty, dynamism, and excellence. Symbiosis Law School, Hyderabad is founded on pillars of expertise, justice, and service and is committed to impart quality legal education conforming to acclaimed International Standards.

ABOUT CYBERSECURITY CENTER OF EXCELLENCE

The Cybersecurity Center of Excellence (CoE) is a joint initiative between the Government of Telangana and the Data Security Council of India (DSCI). In order to promote innovation, entrepreneurship, and capability building in the Cybersecurity ecosystem, the Government of India established it as a non-profit organization. CoE collaborates with organizations across industries, government agencies, universities, R&D centers, and user groups. CoE is committed to making cyberspace safe, secure, and trusted by establishing best practices, standards, and initiatives. India's premier industry body for Cybersecurity is DSCI.

www.ccoe.dsci.in

ABOUT THE CENTRE FOR SPECIALISATION FOR CYBER LAW STUDIES

Centre for Specialisation in Cyber Law studies (CSCLS) of Symbiosis Law School, Hyderabad, is an in-house centre established in 2018 with the aim of educating, researching, and innovation the field of Cyber Law. The Centre focus on different aspects of cyber law through research, events and programmes. The centre works with the aim of propagating the knowledge of rights and duties that a person needs to be aware of while navigating through the cyberspace. Centre for Specialisation in Cyber Law Studies makes it a point to provide the knowledge of cyber security not just to the students of law but to everyone possible in order to enable a future without despair caused by misuse of cyberspace.

ACKNOWLEDGMENT

The Authors would like to thanks and appreciate the opportunity presented to us by CCOE – DSCI to work and present our white paper for the upcoming CCoE - DSCI Chapter Meet on the theme "Data Privacy & Data Protection: Challenges & Solutions". We would also like to thank our Director at Symbiosis Law School, Hyderabad Dr. Santosh Aghav and Deputy Director Dr. Anuradha Binnuri for their constant support and guidance and for allowing us to take up this opportunity.

CONTENTS

EXECUTIVE SUMMARY

The Digital Personal Data Protection Act, 2023 is an ambitious step forward for data protection and privacy in cyberspace of individuals in India. However, the Act remains ambiguous with respect to a multitude of aspects concerning data privacy and protection.

Focusing on the healthcare sector, this Study identifies four key issues with respect to the implementation of the Act in the healthcare industry: Classification and Categorization of Data, De-Identification of Data for research and Development, Reasonable Security Measures and Cross-Border Transfer of Data. The Study analyses these issues in the global context, by considering its global counterparts in legislation, such as the European Union's General Data Protection Regulation. The Study provides for a review of the provisions of the newly accepted Act and provides suggestions and conclusions for the better implementation of key principles underlining the Act.

INTRODUCTION

"Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation."[1]

This was stated by the current Chief Justice of India, Justice DY Chandrachud, as he gave one of the most important judgements in India's judicial history. He was part of a five-judge bench that presided over the case ***K.S. Puttuswamy v. Union of India***[2]**,** also known as the 'Privacy Verdict', which changed the status of privacy in India. This case has acted as a precedent not only in India but in various countries around the world.

Before the *Puttaswamy* judgement, however, the concept of privacy was merely an afterthought. The question of the Right to Privacy was first brought up in 1948 during the constitutional assembly debates, where an amendment was proposed to prevent unreasonable search-and-seizure[3]. However, this was never added to the constitution. For a long time, the Indian judiciary did not recognise the right to privacy as a constitutional right.[4] This trend continued until ***Govind v. State of Madhya Pradesh and Anr***[5], where the Supreme Court finally upheld that the encroachment into a person's privacy shall be deemed 'unconstitutional', if rules and regulations pertaining to surveillance are ignored. Only with the Puttaswamy judgement was the Right to Privacy firmly established as a fundamental right under Part III of the Indian Constitution[6].

Following the *Puttaswamy* Judgement, the Shri Krishna Committee led by Justice BN Srikrishna was formed in 2017 to identify issues related to data protection, suggest remedies and methods to counter them and draft a data protection bill for the first time in Indian history. The Committee

---

[1] Bhaskar A, 'Key Highlights of Justice Chandrachud's Judgement in the Right to Privacy Case' (*The Wire*, 27 Aug 2017) <https://thewire.in/law/justice-chandrachud-judgment-right-to-privacy> accessed 23 September 2023

[2] 2017 10 SCC 1

[3] Team SCO, 'Right to Privacy: Court in Review' (*Supreme Court Observer*, 4 July 2017) <https://www.scobserver.in/journal/right-to-privacy-court-in-review/> accessed 23 September 2023

[4] MP Sharma vs Satish Chandra, (1954) 1 SCR 1077; Kharak Singh vs Uttar Pradesh, 1964 SCR (1) 332

[5] (1975) 2 SCC 148

[6] Team SCO, 'Right to Privacy: Court in Review' (*Supreme Court Observer*, 4 July 2017) <https://www.scobserver.in/journal/right-to-privacy-court-in-review/> accessed 23 September 2023

submitted its report and a draft bill, the Personal Data Protection Bill, to the Ministry of Electronics and Information Technology in July 2018[7].

The Personal Data Protection Bill (PDPB)[8] was introduced in the Parliament in 2021. Notably, the PDPB wasn't India's first attempt at privacy legislation and data protection in cyberspace. The IT Act, 2000[9] first forayed into cybercrimes, however it was initially restricted to mostly commercial crimes or criminal offences. With the 2008 amendment[10], the act finally delved into topics such as identity theft, impersonation, offensive or sexual messages and publishing sensitive images without consent, which therefore gave birth to the very idea of consent and privacy in Indian jurisprudence. However, the scope of the IT Act was quite narrow, and it dealt with only a certain cybercrime, and didn't make an effort to expand over the concept of consent, or talk about breach of privacy.

The PDPB defined personal data, introduced the concept of consent of the user to give access to data and process it, defined data fiduciaries, repercussions of non-consensual processing of data, and appropriate redressal mechanisms, along with offences and penalties[11]. The bill also talked about international transfer of data, and certain grounds for processing of personal data without consent[12]. This was therefore, a huge leap in data protection legislation in India, as it covered many aspects of data privacy which were never truly defined or covered.

The PDPB was withdrawn in August 2022, before introducing the Digital Personal Data Protection Bill (DPDPB) in November 2022, with some changes to the PDPB[13]. On August 12th, 2023, DPDPB received Presidential assent and

---

[7] 'A Free and Fair Digital Economy', (*PRS Legislative Research*, 28 July 2018) <https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy> accessed 23 September 2023

[8] The Personal Data Protection Bill 2019

[9] The Information Technology Act, 2000

[10] The Information Technology (Amendments) Act, 2008

[11] Roy A and P Suraksha, 'Data Protection Board to come up within 30 days MoS IT Rajeev Chandrasekhar', (*The Economic Times*, 20 Sep 2023) <https://economictimes.indiatimes.com/tech/technology/data-protection-board-to-be-set-up-within-30-days-mos-it-rajeev-chandrasekhar/articleshow/103804272.cms> accessed 23 September 2023

[12] Ibid.

[13] Krishna N, 'The Digital Personal Data Protection Act, 2023: Some relief but many questions' (*The Times of India*, 3rd Sept 2023) <https://timesofindia.indiatimes.com/blogs/niveditas-musings-on-tech-policy/the-digital-personal-data-protection-act-2023-some-relief-but-many-questions/> accessed 23 Sept 2023

became the Digital Personal Data Protection Act (DPDPA), 2023, India's first legislation dealing privacy and user consent.

With the digitalisation of industries and sectors across India, the need for the protection of data of individuals becomes very important, especially in industries which deal with sensitive information. One such industry is the Healthcare sector, one of the largest in India, evaluated at $372 billion in 2022, which is 2.2% of the nation's GDP[14].

Data pertaining to the Healthcare industry are sensitive in nature and must come under the purview of the data protection. Health, Healthcare and Medical Data are vital personal information about an individual's medical history, records, and other personal health information regarding his general physical or mental well-being. In today's digital world, almost all hospitals, albeit small or large, government-run or private, have a record of an individual's health data stored on a local database. An individual would only consent to give such vulnerable and personal data for two primary reasons, one being that there is a guarantee that such data would not be released or published to any third party and two being such personal data is used to aid the hospital to find a cure for their condition.

The scope of such data is not limited to the data of an individual finding treatment for his condition, but rather it extends to the research and hypothesis testing conducted by Medical Corporations or Hospitals, for that matter, to discover, identify, and classify diseases and their cures. However, such researches can only be conducted with the data provided by persons who have consented, either expressed or implied consent, to give their personal health data for research, provided such data does not reveal personal details of the individual through anonymisation of the data, and the scope of the data given is only related to the health and well-being of the individual.

---

[14] Sarwal R and others, 'Investment Opportunities in India's Healthcare Sector' (*NITI Aayog*, March 2021) <https://www.niti.gov.in/sites/default/files/2023-02/InvestmentOpportunities_HealthcareSector.pdf> accessed 23 Sept 2023

One of the merits of having such data stored virtually, rather than having physical records of data, is the ease of transfer of Medical Data to parties with whom the Data Principal, i.e. the person who consented to give their Health and Medical Data, wishes to share this data. However, data transfer without first being precautious of where and how the data is being transferred to opens the database to numerous threats.

The primary issue that is prevalent in the DPDPA regarding the privacy or protection of Health Data is that there is an absence of such legislation or mention for any protection of the Health Data that is provided by an Individual who is merely looking for a cure for his/ her condition. The Act portrays several ambiguities with respect to the transfer of health data for intra-border and cross-border scenarios, the scope of reasonable security safeguards, the categorization of health data, and the necessity of encryption techniques for medical research. Through this study, the White Paper shall delve into the various ambiguities of the DPDPA Act while taking reference to several privacy legislations from various jurisdictions including Australia, India, The European Union, Singapore, The United Kingdom, and the United States of America. The Study shall then compare the legislations of these countries to India's DPDPA and suggest changes required to better accommodate privacy in the Indian Medical Field.

I – CLASSIFICATION AND CATEGORIZATION OF DATA

A. CLASSIFICATION AND CATEGORIZATION UNDER THE DPDPA

In the current world, the sheer quantity of information exchanged is so high that it is impossible to regulate all data with 100% efficiency. Hence, there is a need to hold different kinds of data to different standards of protection. While it is recognised that the right to privacy concerning personal data is extremely important, it is undeniable that certain types of data hold more value than others[15].

The Healthcare Industry holds a vital role in propelling development in most countries. It deals with extremely sensitive personal data in large volumes. This calls for a higher degree of data protection and more obligations to be placed upon those involved in processing such sensitive data.[16] The measures that can be taken to secure such data include but are not limited to specified data retention periods, prohibition or restriction on processing data, and increased oversight on data processing and retention.

Categorisation of data is a method used to effectively identify and regulate different kinds of data. The recently passed DPDPA does not explicitly categorise data types or distinguish between different kinds of "personal data". It has, however, differentiated between different types of Data Fiduciaries. The Central Government has the power to classify certain Data Fiduciaries or classes of Data Fiduciaries as Significant Data Fiduciaries, and its determination is based on various aspects, including the volume and sensitivity of personal data[17]. According to the Act, these Significant Data Fiduciaries or Classes of Significant Data Fiduciaries will be held to higher standards and meet specific requirements than other Data Fiduciaries. The problem lies in individually identifying these Significant Fiduciaries and determining the extent of their obligation in handling such data.

---

[15] Mark Stone, '2023 Data Classification Overview: Labels & Levels Explained' (*Concentric AI*, 3 April 2023) <https://concentric.ai/the-importance-of-data-classification-levels-and-labels/> accessed 25 September 2023

[16] Romain David and others, 'An Iterative and Interdisciplinary Categorisation Process towards Fairer Digital Resources for Sensitive Life-Sciences Data' (*Nature News*, 5 December 2022) <https://www.nature.com/articles/s41598-022-25278-z> accessed 25 September 2023

[17] DPDPA, s 10

Data categorisation is already prevalent in India through the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, also known as the SPDI Rules, 2011. Rule 3[18] of the SPDI Rules defines Sensitive Personal Data or Information as information relating to passwords, financial information, physical, physiological, and mental health conditions, sexual orientation, medical records and history, biometric information, etc.

The Electronic Health Record (EHR) Standards 2016[19], issued by the Indian Ministry of Health and Family Welfare, is an attempt to standardise different kinds of health data record systems across the country. While these Standards are non-binding, it remains very beneficial in the efficient regulation of particular types of data. Hence, it is important to revamp the scope and ambit of Health Data in order to place additional obligations for the protection of such Data.

B. OVERVIEW OF INTERNATIONAL JURISDICTIONS

UNITED STATES OF AMERICA (USA)

While the United States of America does not have any federal data protection legislation, they enforce privacy standards through other specific legislations and state laws. The Health Insurance Portability and Accountability Act (HIPAA), 1996[20] is one such federal law that ensures the security of healthcare data. The HIPAA Privacy Rule[21] has 18 identifiers for classification as Protected Health Information (PHI). These identifiers are specific and unambiguous.

According to this, PHI is not restricted to purely health-related information but all the supporting identifiers of a person like social security address, specific address, fax numbers, telephone numbers, IP address, web URLs, etc.

---

[18] SPDI, Rule 3
[19] Ministry of Health & Family Welfare, '*ELECTRONIC HEALTH RECORDS (EHR) STANDARDS FOR INDIA 2016*' <https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf> accessed 25 September 2023
[20] Health Insurance Portability and Accountability Act 1996 (hereinafter referred to as HIPAA)
[21] Health Insurance Portability and Accountability Act Privacy Rule 2000 (hereinafter referred to as HIPAA Privacy Rule)

However, studies[22] indicate that these 18 identifiers are still ineffective in protecting data anonymity, which suggests a need for more stringent identifier standards or stronger security measures and legal sanctions[23]. Further, e-PHI[24], which is PHI in digital form, is protected under the HIPAA Security Rule[25]. Implementing supplementary legislation like the Health Information Technology for Economic and Clinical Health (HITECH) Act[26] helps ensure compliance with standards set in previous legislation.

The California Consumer Privacy Act (CCPA)[27] has classified Sensitive Personal Information to include information regarding the consumer's health, biometric information, genetic data, sexual orientation, etc. This classification is similar to that done in GDPR and SPDI Rules. The California Confidentiality of Medical Information Act (CMIA)[28] gives a broader scope to "medical information"[29] compared to HIPAA and also increases the liability of a person disclosing such information to not just a fine, as in the case of HIPAA, but also legal action.

Notably, the CCPA and CMIA are state legislations and are not binding in other territories. However, it serves as an example of how state legislation can cater to the specific needs of different industries while complementing federal law. The combination of classification of data in general legislations like CCPA combined with sector-specific legislations like the HIPAA and CMIA makes US Healthcare data regulation very efficient.

---

[22] Steven L Clause and others, 'Conforming to HIPAA Regulations and Compilation of Research Data' (*American Journal of Health-system Pharmacists*) <https://pubmed.ncbi.nlm.nih.gov/15160778/> accessed 25 September 2023

[23] Nass SJ, Levit LA and Gostin LO, 'HIPAA, the Privacy Rule, and Its Application to Health Research', Beyond the HIPAA privacy rule: Enhancing privacy, improving health through research (National Academies Press 2009)

[24] Alexis Porter, 'A Guide to Types of Sensitive Information' (*BigID*, 8 May 2023) <https://bigid.com/blog/sensitive-information-guide/> accessed 25 September 2023

[25] 'DPDPB and GDPR Data Classification' (*Tsaaro*, 28 July 2023) <https://tsaaro.com/blogs/dpdpb-and-gdpr-data-classification/#:~:text=GDPR%20and%20Data%20Classification,%2C%20union%20membership%2C%20and%20more.> accessed 25 September 2023

[26] Health Information Technology for Economic and Clinical Health Act 2009

[27] The California Consumer Privacy Act 2018

[28] The California Confidentiality of Medical Information Act 1981

[29] Andrew Serwin and others, 'California Expands Scope of Confidentiality of Medical Information Act' (*DLA Piper*) <https://www.dlapiper.com/en-jp/insights/publications/2022/11/california-expands-scope-of-confidentiality-of-medical-information-act> accessed 25 September 2023

European Union (EU)

The General Data Protection Regulation (GDPR)[30] is a universally celebrated data legislation that is binding on the European Union and European Economic Area (EEA) countries. Article 4 of GDPR defines "Personal data" while Article 9 of GDPR[31] prohibits processing special categories of personal data or 'sensitive data', including data concerning racial or ethnic origin, religious beliefs, genetic data, biometric data, health, sexual orientation, etc. The statute establishes that these special categories of personal data merit a higher degree of protection by adding restrictions[32] on them and placing more obligation[33] on those authorised to process such data[34]. It is also essential to recognise that the GDPR is supplemented with national laws[35] that elaborately deal with medical confidentiality in most EEA countries.

Singapore

In Singapore, the Personal Data Protection Act (PDPA) provides a basic standard for the regulation of personal data. The term "Personal data"[36] is only loosely defined under the Act. It does not distinguish between different kinds of personal data[37]. However, the PDPA is meant to be an elementary guide for data legislation as it is intended to operate alongside sector-specific legislation like the Healthcare Services Act [38] and its regulations[39]. Further, the 2015 National Guidelines for Retention Periods for Medical

---

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 (hereinafter referred to as GDPR)

31 GDPR, Art 9

32 GDPR, Art 22(4), Art 27(2)

33 GDPR, Art 30(5), Art 35(3), Art 37, Art 47

[34] Vera Lúcia Raposo and Tomás de Brito Paulo, 'Data Classification' (*EuroGCT,* 14 March 2023) <https://www.eurogct.org/research-pathways/public-involvement-and-data/data-protection/data-classification> accessed 25 September 2023

[35] Johan Hansen and others, 'Assessment of the EU member states' rules on health data in the light of GDPR' (*European Commission*) <https://health.ec.europa.eu/system/files/2021-02/ms_rules_health-data_en_0.pdf> accessed 25 September 2023

36 The Personal Data Protection Act 2012, s 2(1) (hereinafter referred to as PDPA)

[37] Simon Chesterman, "After Privacy: The Rise of Facebook, the Fall of Wikileaks, and Singapore's Personal Data Protection Act 2012" (2012) Singapore Journal of Legal Studies 391 <https://www.jstor.org/stable/24872218> accessed 24 September 2023

[38] The Healthcare Services Act 2020

[39] The Healthcare Services (General) Regulations 2021

Records[40], issued by the Ministry of Health, categorised the different kinds of medical records and dictated different data retention periods and risk management strategies.

C. SUGGESTIONS

When analysing the International Legislations concerning health data, under the US's HIPAA, Health Data is specifically categorised as PHI under a sectorial regulation allowing for the government to effectively legislate on detailed security measures especially tailored to the healthcare industry. However, while India does not have specific sectorial Data Protection Regulations, EU's GDPR specifically differentiates between Personal Data and Sensitive Data while also placing additional obligations on organizations processing such sensitive Data. Similarly, in Singapore, although the PDPA provides for a general overview on the scope of Personal Information, guidelines issues by concerned ministries, such as the Ministry of Health, have incorporated guidelines specifically categorizing certain Health Data.

It can be observed that the model of data legislation that works in most other countries is where a federal law sets out the basic structure of data legislation and uses sector-specific regulation to cater to the needs of each industry. The flexibility that comes with sectoral regulation is essential in dealing with the dynamic field of cyber law and data protection.[41] With regard to health-related data, having more specific categorisation and security standards will be easier in identifying breaches[42] and addressing them effectively.[43]

---

[40] 2015 NATIONAL GUIDELINES FOR RETENTION PERIODS OF MEDICAL RECORDS (*Ministry of Health Singapore,* 28 January 2015) <https://www.moh.gov.sg/docs/librariesprovider5/licensing-terms-and-conditions/national-guidelines-for-retention-periods-of-medical-records-(dated-28-jan-2015).pdf> accessed 25 September 2023

[41] 'The Protection of Personal Data in Health Information Systems- Principles and Processes for Public Health' (*World Health Organization*, 1 January 1970) <https://apps.who.int/iris/handle/10665/341374> accessed 25 September 2023

[42] Manny Rivelo, 'Council Post: Why the Data Security Lifecycle Is Essential for Reducing Cost and Risk' (*Forbes*, 1 May 2023) <https://www.forbes.com/sites/forbestechcouncil/2023/05/01/why-the-data-security-lifecycle-is-essential-for-reducing-cost-and-risk/?sh=3bae3a4bcf52> accessed 25 September 2023

[43] 'Data Classification (Data Management): A Complete Overview' (*Spirion*, 9 July 2023) <https://www.spirion.com/data-classification/> accessed 25 September 2023

It is suggested that India adopt a similar system where the DPDP Act, along with other existing cyber legislation, can give a generalised classification of data and establish standards of protection, while specific legislations or sectoral regulations can dictate actual categorisation of data according to the requirements of various industries. The DISHA guidelines[44] were a step towards establishing such a system in the healthcare sector. However, whether the DISHA or any other medical sector-specific guidelines will gain any force in law remains to be seen.

[44] 'DISHA GUIDELINES' (*Ministry of Rural Development*) <https://dishadashboard.nic.in/guidelines> accessed 25 September 2023

II – De-Identification of Data for Research and Development

A. De-Identification of Data for Research and Development under the DPDPA

Since Covid-19, the healthcare industry has been going through a significant digital transformation in India and around the globe. This has provided express protection to the data of the individuals involved. Healthcare providers generally use electronic health records (EHRs) solely for clinical care purposes.[45] Personal and sensitive information that can identify individuals must be effectively made anonymous. De-Identification Techniques involve removing identifiers of individuals and is commonly done through anonymization or pseudonymization. Frequently, raw data is de-identified for research use, with a thorough evaluation of the risks associated with re-identification and its overall usefulness.[46]

It must be highlighted that the present DPDPA does not define or elaborate on the topic of de-identification. However, while the concept as a whole is absent in the DPDPA, it was proposed in PDPB introduced in 2019 under section 3(16)[47]. This Section defines 'de-identification' as the "*means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal*". Moreover, Section 50(6)(m)[48] of the bill provided with the appropriate authority to establish a code of practice for methods of de-identification and anonymisation, which has been excluded from the ambit of the DPDPA.

---

[45] Z Zuo and others, "Data Anonymization for Pervasive Health Care: Systematic Literature Mapping Study" (2021) JMIR Med Inform 9(10) <https://preprints.jmir.org/preprint/29871?__hstc=102212634.82ff711470c0fa8b09a67872b497f759.1695654257952.1695654257952.1695654257952.1&__hssc=102212634.1.1695654257953&__hsfp=597160832> accessed 23 September 2023

[46] Zhicheng He, "From Privacy-Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law", (2023) DISO 2 <https://doi.org/10.1007/s44206-023-00043-5> accessed 23 September 2023

47 PDPB, s 3(2)

[48] PDPB, s 50(6)(m)

The term 'Anonymization' refers to the process of converting any data, especially sensitive information in cases of data privacy, into anonymous information such that identification of individuals to whom the data is related is not identifiable.[49] Anonymous Information has been defined under Recital 26[50] of GDPR as "*information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.*"

On the other hand, Article 4(5) [51] of the GDPR explains the concept of Pseudonymisation of data as "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*"

From the definitions of these two techniques, it can be understood both techniques aim to mask personal information through the removal or encryption of personal data. However, the scope of Anonymization is much higher wherein, Personal Identifiers are deleted to remove the possibility of re-identification of data. Whereas in Pseudonymisation, data can be re-identified with a specific key or method[52].

Research and development in the field of biomedicine and biotechnology requires large sets of data to study more from. These are essential in improving the standards of life-saving medicines and techniques. The Healthcare industry deals with EHRs, commonly categorised as sensitive personal data which are used for a multitude of purposes. With the increasing use of digital technology and artificial intelligence, the data

---

[49] Dong Li, and others, "Permutation anonymisation" (2016) J Intell Inf Syst 47. <https://doi.org/10.1007/s10844-015-0373-4> accessed 23 September 2023.
[50] GDPR, Recital 26.
[51] GDPR, Art.4(5)
[52] P. L. M. K. Bandara, and others, *"Evaluation of Re-identification Risks in Data Anonymization Techniques Based on Population Uniqueness,"* (2020) 5th International Conference on Information Technology Research (ICITR) <https://doi.org/10.1109/ICITR51448.2020.9310884> accessed 24 September 2023

collected by the healthcare industry has become more vulnerable.[53] Such sensitive data are used for research and development purposes by different authorities, which may compromise the privacy of the data principal. This raises the concern of Data Protection for Research purposes under the DPDPA. Resultingly, there is a need to define and establish de-identification techniques under the DPDPA to effectively ensure that data for research purposes are well protected.

B. OVERVIEW OF INTERNATIONAL JURISDICTIONS

EUROPEAN UNION (EU)

When examining the EU's GDPR, pseudonymisation under the regulation is promoted and encouraged as a mode for maintaining lawfulness[54] and security[55] in the processing of data for purposes other than that for which the personal data have been collected is not based on the data subject's consent. Compliance of safeguarding data through the technical measure of Pseudonymisation and data protection by design also helps in achieving the principle of data minimisation[56].

When examining the scope of the use of Personal Information for Research Purposes, Article 89(1) of the GDPR[57] provides certain exemptions of such Personal Information from Data Subject Rights, however, it is necessary that appropriate safeguards are implemented for the protection of such Data including pseudonymisation. Hence, the GDPR effectively encourages the use of pseudonymisation for research purposes as a means of effective security safeguards.

However, with respect to Data Anonymization, the GDPR has given no legal status to it as recital 26[58] states that the act only applies to data of an

[53] L Ferretti and others, "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing" (2020) Science 368(6491) <https://www.science.org/doi/10.1126/science.abb6936> accessed 23 September 2023.
[54] GDPR, Art. 6(4)(e)
[55] GDPR, Art. 32(1)(a)
[56] GDPR, Art.25(1)
[57] GDPR, Art.89(1)
[58] GDPR, Recital 26

identifiable individual and not anonymous data. This effectively removes anonymous information from the ambit of the GDPR and hence, anonymization of data is seen to be an effective method of de-identification as the permanent remove of personal identifiers will remove the data's scope as Personal Information under the GDPR, thereby, promoting the application of anonymization under the GDPR.

UNITED STATES OF AMERICA (USA)

The US's HIPAA sets standards for de-identification of PHI under section 164.514[59] through expert determination and safe harbor. Under this, "*Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information*."[60] Thus, de-identified data us removed from the scope of identifiable health information.

Under this act, the Expert Determination method states that a covered entity can consider health information as not individually identifiable if a qualified expert determines, through established statistical and scientific methods, that there is a very low risk of re-identification.[61] Whereas, under the Safe-harbour method, a covered entity must either remove specific identifiers like names, addresses, dates, etc., or ensure they have no knowledge that the information could still identify an individual.[62]

These two standards of de-identification allow covered entities to ensure adequate de-identification through defined scope under the HIPAA, allowing for effective de-identification with comparatively lower risks.

[59] HIPAA, s 164.514
[60] HIPAA, s.164.514(a)
[61] HIPAA, s.164.514(b)(1)
[62] HIPAA, s 164.514(b)(2)

UNITED KINGDOM (UK)

The UK's Data Privacy Act, 2018 (DPA) regulates the processing of information in line with the GDPR. Section 171[63] of the act also defines de-identified data as Personal Data that "*has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject*."

On the other hand, Section 19[64] of the act, provides for the exemptions on the processing of data for research and statistical purpose. On the lines of Article 89 of the GPDR[65], the process may have derogations on certain rights of individuals including right of access, right to rectification, right to restriction of processing & right to object. However, it is still necessary for the data to be secured and protected so as to avoid any substantial damage or distress likely to cause harms to the rights and freedoms of individuals.

In the case of **R (on the application of the Department of Health) v. Information Commissioner**[66] **,** the question of disclosing the data used for generating reports and statistics after anonymisation was debated. Considering the exemption of anonymous data from the ambit of GDPR and the concept of personal data under DPA, the court held that anonymous data, which cannot lead to the identification of the individual, cannot be considered as personal data and thus can be disclosed on rising of substantial questions.

For effective administration of data privacy laws, Information Commissioner's Office (ICO) release code of practice which has resulted in clear and better understanding and application of laws on data processing involving data anonymisation. The ICO released two Codes regarding Anonymisation which gives guidance[67] and a code of practice[68] for managing personal data. The National Health Services Foundation Trust

[63] DPA, s 171
[64] DPA, s 33
[65] GDPR, art 89
[66] *R (on the application of the Department of Health) v Information Commissioner* [2011] EWHC 1430 (Admin)
[67] Information Commissioner's Office, 'Introduction to Anonymisation: Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance' (*ICO*, 2021)
[68] Information Commissioner's Office, 'Anonymisation: Managing data protection risk code of practice' (*ICO*, 2012)

also releases policies and regulations to administer anonymisation of data in the country. The NHS Foundation Trust also laid down detailed policies[69] and procedures[70] for pseudonymisation and anonymisation of data.

Hence, although the DPA and UK's GDPR are the main regulations pertaining to Data Protection, these legislations have been supplemented with policies and guidelines for the effective handling and de-identification of data by organizations.

C. SUGGESTIONS

After analysing the international jurisdictions and existing legislation recognizing and regulating anonymisation of data, it is clear that the need for legislations governing de-identification cannot be underestimated. It is of paramount importance for the DPDPA or its subsequent legislation to address the issue of de-identification of data. By not laying down procedure for the same, the act will either risk the privacy of individuals without anonymisation or exempt the use of sensitive personal data for research and development purposes, stifling progress. While the scope of anonymization has been exempted from the GDPR, pseudonymization has remains within the scope of the GDPR as well as the regulations of US & UK.

It is suggested that an amendment to the DPDPA must be made with reference to such existing laws to incorporate laws on anonymisation of data, especially in the healthcare industry. The scope and definition of de-identification must be established under the DPDPA, like it similarly was in the PDPB. It is also suggested that clear standards defined through rules or guidelines regarding the use of Data for Research Purposes under the DPDPA. Moreover, the Central Government must establish specific guidelines on uniform methods and standards of de-identification that would help promote the effectiveness of security of Data for Research and Development

[69] National Health Services Foundation Trust, 'Anonymisation of Data (Pseudonymisation) Policy and Procedure' (*NHS*, 2017).
[70] National Health Services Foundation Trust, 'Pseudonymisation and Anonymisation of Data – Procedure' (*NHS*, 2019).

in the healthcare industry. Implementing these suggestions would prove to be immensely beneficial to individuals who's data have been used for Research Purposes by mandating organizations to adhere to specific de-identification measures.

III – Reasonable Security Measures

A. Reasonable Security Measures under the DPDPA

One of the underlying objectives of the DPDPA was to ensure adequate and reasonable security safeguards to Personal Data collected by organizations in India. The rationale behind the implantation of such security measures has originated from the development of the Right to Privacy in India[71] and the Right of Individuals to protect their personal data. The latter Right has been expressly recognized under the preamble of the DPDPA[72] and has seen growing recognition on a global scale with many governments enhancing Data Protection Regulations with the aim of preserving this Right[73]. Hence, the Protection of Personal Information and Data from Potential Data Breaches continues to be a significant challenge globally with new regulatory mechanisms attempting to reduce the rate of such Breaches.

Data Breaches are widely common occurrences in the Global World and can happen from (1) actions by careless employees with lack of training and who fail to follow proper procedure, (2) hackers who attempt to gain access to protected databases or even (3) individuals who steal unprotected devices[74]. Apart from the abovementioned cases, there are several other situations that can result in potential security concerns and data breaches. However, while preventing Data Breaches are essential to protect individuals, organizations that are victims to Data Breaches are prone to sever reputational damages and financial losses[75]. As a result, preventing potential security breaches remains an important challenge for individual, governments and organizations.

According to the Cost of a Data Breach Report 2023, conducted by IBM, Phishing and Stolen compromised credentials were reported to be the two

---

[71] Justice K.S. Puttuswamy & Anr v. Union of India 2017 10 SCC 1
[72] DPDPA, preamble
[73] GDPR; HIPAA; PDPA
[74] OECD, *The OECD Privacy Framework* (2013) <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 24 September 2023
[75] Long Cheng, Fang Liu & Danfeng Yao, 'Enterprise data breach: causes, challenges, prevention, and future directions' [2017] 7 Wires Data Mining and Knowledge Discovery 1.

most common initial attack vectors that was responsible for 16% and 15% of Data Breaches respectively[76]. Moreover, phishing attacks resulted in an average cost of USD 4.76 million per Data Breach and took on average 293 days to identify and contain a data breach caused by a phishing attack. Hence, this report underscores the importance of ensuring adequate and reasonable security measures amongst organizations as well as sufficient employee training.

The DPDPA bestows on Data Fiduciaries several obligations out of which, one of the most significant ones in terms of Security is under Section 8(5) which states,

"8. (5) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach."[77]

From a bare reading of the DPDPA, the scope for ensuring reasonable security for the protection of personal information seems drastically diminished from the act's predecessor, the Personal Data Protection Bill, 2019. Under this Bill, Section 24[78] proposed to place obligations on implementing security measures adequate to the sensitivity and nature of the data while mandating the use of certain steps including de-identification, encryption and steps to prevent misuse, modification while protecting the integrity of the data. Furthermore, clause (2) of the Bill also places an obligation for periodic reviews of security measures which furthered the goal of Security measures.

Prior to the implementation of the DPDP, the SPDI Rules was India's primary Data Protection Regulation, under which Rule 8 obligated Body Corporates (any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities) to incorporate reasonable security measures and provided for the 'The

[76] IBM, *Cost of a Data Breach Report* (2023) <https://www.ibm.com/reports/data-breach> accessed 24 September 2023
[77] DPDPA, s 8(5)
[78] PDPB, s 24

international Standard IS/ISO/IEC 27001' as one such practice that would fulfil the criteria under Rule 8[79]. The rules also mentioned that body corporates may resort to other best practices duly approved and notified by the Central Government for effective implementation[80]. However, no such rules have been notified by the Central Government.

While the DPDPA does not contain any specification with respect to the term 'Reasonable Security Measures', there exists no clear understanding as to the scope of what is reasonable and what are measures that are deemed unreasonable. In regard to the Healthcare Industry, where Privacy of information is vital, there is an apparent ambiguity on the face of the DPDPA. As Data in the healthcare industry is considered as 'sensitive data', it is important to redefine the scope of reasonable security measures.

B. OVERVIEW OF INTERNATIONAL JURISDICTIONS

UNITED STATES OF AMERICA (USA)

In the US, the HIPAA is the main Federal Legislation that governs the handling of Data in the Healthcare Industry. Under this, Electronic PHI (ePHI) is protected in Part 164, Subpart C concerning Security Standards for the Protection of Electronic Protected Health Information (Security Rule)[81]. The HIPAA ensures security and compliance by requiring the implementation of certain physical, technical, and administrative safeguards including confidentiality, integrity, and security of ePHI. The Act provides for a flexible approach towards adopting security measures allowing entities to implement reasonable security measures in terms of the entity's size, complexity, infrastructure, hardware, security capabilities, costs of security, etc. Under the various heads of safeguards, the Act details on various types of measures to be applied which may either be mandatory and required or may be addressable for which the entity is to assess whether the requirement is reasonable and appropriate. However, it is essential that an

[79] SPDI, rule 8
[80] SPDI, rule 8(4)
[81] HIPAA, s 164

entity reviews its security procedures regularly to stay compliant with the Act.

Under Administrative Safeguards, entities are required to implement policies and procedures to prevent, detect, contain, and correct security violations. The Act requires entities to (1) Conduct Risk Analysis, (2) Implement Security Measures, (3) apply appropriate Sanctions against workforce that fail to comply with security procedures, (4) conduct regular Information system activity review, (5) employ policies to ensure appropriate access to ePHI amongst the workforce, (6) implement security awareness and training program for all members of its workforce, (7) Identify and respond to security incidents, (8) Establish Data Backup Plan, (9) establish Disaster Recovery Plan, (10) Document written contract for handling of ePHI on behalf of the entity. The Act also provides for several other addressable measures to be taken by Entities if necessary.[82]

With respect to Physical Safeguards, entities are required to (1) establish policies and procedures for effective discharge of functions for specific workstations, (2) Implement physical safeguards for all workstations accessing ePHI, and (3) Implement policies and procedures to address the final disposition of ePHI. Similar to the Administrative Safeguards, the Act also provides for addressable measures.[83]

Finally, with respect to the Technical Safeguards, entities are required to (1) Assign a unique name and/or number for identifying and tracking user identity, (2) Establish procedures for obtaining necessary electronic protected health information during an emergency, and (3) Implement Audit Controls.[84]

HIPAA, while covering all the significant aspects and policies that are essential for Entities to abide by for security, it also provides the utmost level of flexibility for the incorporation of security measures to ensure a high standard of security and protection. While reasonable security measures

[82] HIPAA, s 164.308
[83] HIPAA, s 164.310
[84] HIPAA, s 164.312

are mandated, it provides less ambiguity as to what constitutes reasonable and ensures that entities cover several grounds to be compliant with the Security Rule of the HIPAA.

European Union (EU)

Article 32 of the GDPR[85] discusses the aspect of Security in the processing of Data. Under this, Data Controllers are obligated to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Unlike the HIPAA, the GDPR does not go in-depth with respect to a security checklist but defines an inclusive list of appropriate measures including (1) the pseudonymisation and encryption of personal data, (2) ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services, (3) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and (4) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. Hence, although not exhaustive, the GDPR reduces the lack of ambiguity with respect to 'reasonable' and 'appropriate' security measures by providing an inclusive checklist.

Australia

The main legislation governing Data in Australia is the Privacy Act 1988[86]. Under this Act, Chapter 11 deals with the Security of Personal Information and notes that a regulated entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. Furthermore, the Act also mandates entities to destroy or de-identify information when the information is no longer required[87]. While the security clause simply denotes

[85] GDPR, Art 32
[86] The Privacy Act 1988
[87] The Privacy Act 1988, chapter 11

'reasonable' steps and creates high ambiguity in determining what is reasonable, the Privacy Act must be read with the Australian Privacy Principles Guidelines (APPG)[88]. The APPG although non-binding in nature, provides for methods and guidelines on compliance with the Privacy Act. Under this, the term reasonable has been elaborated to include various steps such as (1) governance, culture and training, (2) internal practices, procedures and systems, (3) ICT security, (4) access security, (5) third party providers (including cloud computing), (6) data breaches, (7) physical security, (8) destruction and de-identification, and (9) standards. Although non-binding, the guidelines have drastically reduced the ambiguity surrounding the term 'reasonable' in the Australian Privacy Landscape.

C. SUGGESTIONS

As iterated in the abovementioned paragraphs, the scope of the DPDP with respect to 'reasonable' security safeguards is ambiguous. The Act only obligates Data Fiduciaries to implement reasonable security safeguards to prevent personal data breaches but does not provide clarity as to the specification of what is reasonable. Unlike the DPDP, the HIPAA provides for a detailed checklist of requirements and addressable measures that are to be taken by covered entities spanning over several measures. Moreover, EU's GDPR and Australia's Privacy Act and guidelines also provide for certain checklists and inclusive lists of reasonable security measures and suggested measures that may be undertaken for entities to be compliant with the Data Protection Regulations. While it is understood that new forms of security advancements are developing every day and redefining the scope of reasonable security measures, it is important to provide clarity as to what may constitute as 'reasonable'.

It is suggested and recommended that the DPDPA is amended to provide an inclusive list of measures that may be undertaken by Data Fiduciaries

[88] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (2022) <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines> accessed 24 September 2023

including technical and organizational measures to reduce the gap of ambiguity on what is reasonable. Moreover, it is further suggested that specific and detailed guidelines may be released by the Central Government after considering submissions, if any, made by stakeholders, on what constitutes reasonable security measures and a basic checklist for organizations in the Healthcare Industry. Doing the same would ensure uniformity in Data Protection and Security Measures while also reducing the ambiguity on what constitutes as 'reasonable' security safeguards and measures.

IV – Cross-Border transfer of Data

A. Cross-Border Transfer of Data under the DPDPA

Cross-border transfer of data refers to the flow of personal data from one country to another. When the personal data of a person is transferred from one country to another country, or territory which is outside its jurisdiction, that flow, or transfer, of data is referred to as cross-border flow of data. This movement of data takes place across servers of one country to another.[89] A primary example of this are businesses that operate globally such as hotels, car manufacturers, freight and logistics enterprises and restaurant chains benefit from data analytics that allow them to reach more customers, improve customer experiences and work more efficiently. Businesses must pool large amounts of data from their centers around the world to accomplish these goals.[90]

The DPDP Act has made cross-border transfer of data significantly easier for data fiduciaries by simply removing restrictions on such flow of data. S. 16 of the Act[91] serves as an enabling clause for cross-border flow of data by making all such movements of data as lawful unless the Central Government explicitly restricts transfer of data to countries or territories outside of India. This effectively legalizes all transfers of data to territories outside India and all other countries subject to the exception that such territory has not been explicitly excluded.

While the provision for cross-border data transfer in the Act certainly makes the process of sharing data and information easier, it also raises some serious concerns regarding the safety of data. Global data flow, as reported in the World Development Report by the World Bank was 3 zettabytes, which is roughly 3 trillion gigabytes. To put it into perspective, it translates roughly

---

[89] Cross Border Data (BSA, 1 February 2023) <https://www.bsa.org/policy-issues/cross-border-data#:~:text=BSA%20supports%20international%20data%20transfer,transfer%20provisions%20in%20trade%20agreements> accessed 23 September 2023

[90] Cross-Border Data Flows (BSA, 1 February 2023) <https://www.bsa.org/policy-filings/cross-border-data-flows> accessed 23 September 2023.

[91] DPDPA 2023

into the equivalent of 100,00 gigabytes per second globally. The number was expected to reach 150,000 gigabytes of traffic per second.[92] When one understands the sheer size and amount of data and personal information of persons flowing across the world at such a humongous rate, it is obvious why there is a need for provisions of security and safety of the data being transferred. The DPDPA has not specified any measures for protection of data being transferred to extraterritorial jurisdictions. S. 16(2)[93] of the Act mentions that it would not affect the applicability of any law providing for a higher degree of protection for or restriction on transfer of personal data outside India. However, the Act itself has no provisions or security measures. Furthermore, cross-border transfer of data must also be looked at along with provisions for data localization: if a corporation or any organization provides for data to be stored only in local servers, provisions for cross-border transfer become redundant. For example, when RBI published its data localization policy in 2018 that required all payments system data to be stored in India, it raised concerns about how cross-border transfer of data in the context of international transactions would be treated. Cases such as these raise the concern of Data Storage in International Jurisdiction, data mirroring and lack of measures to address any conflicts that may arise thereof. The DPDP Act remains silent on all such concerns.

Finally, another concern that has been raised is that if each nation has its individual, country-specific policies and legislation, how would disputes relating to cross-border flow of data be resolved, since each country would insist on their own laws being upheld. A lack of an overarching global institution or framework that serves as a watchdog to cross-border flow of data coupled with the near non-existent provisions in the DPDPA is indeed concerning for individuals whose data is being processed and transferred across international borders.

In the healthcare sector, cross-border flow of data is absolutely essential and of immense significance. Health data is used for two purposes, i.e., primary and secondary. The primary usage of health data is direct patient

[92] Crossing Borders <https://wdr2021.worldbank.org/stories/crossing-borders/> 23 September 2023.
[93] DPDPA, s 16(2)

care. The data of a person used to treat the person himself is direct patient care. If a patient was to transfer to a different hospital or medical institute in a different country, his data would be transferred to the hospital situated in another country. This is the primary use of healthcare data, and how it functions with cross-border flow of data. The secondary use of health data refers to the data being utilized for a different purpose than the one which it was collected for. This can be administrative data, insurance claims, patient health data etc. used for research and improving quality of treatments.[94]

B. OVERVIEW OF INTERNATIONAL JURISDICTIONS

EUROPEAN UNION

The EU has three tests based on which it determines whether data can be shared with another country or not. The GDPR, while allowing cross-border flow of data, has regulations for the same. Its regulations for transfer of data to nations outside the EU are subject to certain tests. The first of these is the adequacy test, which is based on a thorough assessment on whether the third country has appropriate legal safeguards for the protection of data being transferred, i.e., whether the country's data protections laws are adequate. Following this test, there are Standard Contractual Clauses (hereinafter "SCCs") and Binding Corporate Rules (hereinafter "BCRs"). The European Commission sets out certain SCCs which provide sufficient safeguards on the data being transferred. These SCCs are set out on EU controllers who transfer the data. For transfer of data between different company entities, the BCRs come into play. BCRs are legally binding rules approved by a supervising authority which regulates the transfer of personal data within groups of enterprises or undertakings that are engaged in a joint economic activity.

---

[94] Empowered by The Cloud: How Cross-Border Health Data Flows Can Create Value For Patients And Boost Health System Efficiency (HIMSS, 1August 2023) <https://www.himss.org/resources/empowered-cloud-how-cross-border-health-data-flows-can-create-value-patients-and-boost accessed 24 September 2023> 23 Septembr 2023.

While these tests are of paramount importance to ensure that personal data of individuals which flows one country to another stays protected and their privacy remains intact, the flaws in them are also very visible: if a patient is transferring to a healthcare institute in a different country, but the laws of that country fail to stands up to EU's stringent standards, the flow of data would be hampered. Considering that the healthcare industry works primarily for the betterment of the global society, wherein health data would be used for research and for the advancement of medical sciences and R&D, sharing of data would instead be invaluable to society at large. Furthermore, reused health data, which is data being utilized for a different purpose than originally collected for, i.e. data utilized for the secondary purpose, remains anonymous. Since reused data is generally owned by the hospitals and medical institutes, such data can be stripped completely of individual identifiers.[95] This maintains anonymity for the persons whose data it may have been, and as such, the flow of this data would not lead to breach of any individua's privacy. While EU's adequacy tests and compliance mechanisms may seem excessive, it is critical to understand that they are also absolutely essential to maintain privacy of individuals and for data protection.

In Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems[96], popularly known as the Schrems II decision, the CJEU upheld the validity of the EU's SCCs, and held the US-EU Privacy Shield as being invalid. The CJEU, in deciding the validity of SCCs in cross-border transfers of data, reiterated Article 44 of the GDPR[97] which stated that the level of protection of persons when their natural data is being transferred cannot be undermined. The CJEU also stated that if protection guarantees within the EU cannot be ensured while transferring personal data to another country, then supervising authorities must suspend or prohibit data transfers to such countries. There is another visible fundamental flaw in this with relation to the healthcare industry: the tests in the EU are to be conducted at the time

[95] Id.
[96] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., 2020 EU:C:2020:559 (July 16, 2020).
[97] GDPR

of transfer of data, unless there is an adequacy report by the EU on that country. However, with respect to SCCs and BCRs, compliance must be observed throughout the transferring of data. If a patient is being taken to a different country for immediate treatment, and it is observed that the private hospital or facility the patient is being taken to, the flow of his health data will be necessarily suspended, severely impeding his treatment and his health, potentially endangering his life as well. As for research purposes, suspension of data severely restricts medical growth and advancement in a country as well, which is extremely detrimental for society and populace of that country. A balance must be sought between strict compliance and emergent needs in the healthcare industry.

UNITED STATES OF AMERICA (USA)

Under US's HIPAA, Entities covered are bound to ensure protection of privacy of individuals and security of protected health information. Entities are bound to implement safeguards towards the same. HIPAA does not prohibit cross-border transfers of data and instead, has a "Privacy Rule" which talks about privacy and protection of health data.[98] The provisions in HIPAA are extremely similar to those of GDPR, the key difference being that HIPAA applies only to covered entities, which are regulated healthcare entities and associated businesses, whereas GDPR has an EU-wide application on every entity and natural person. HIPAA also states that organizations must ensure that they have the necessary safeguards and agreements in place to maintain security of protected health information.

C. SUGGESTIONS

While the DPDPA explicitly allows cross-border transfer of data, it also contains a similar clause under S. 16(2)[99] that laws which provide for higher

[98] Bradford L, Aboy M and Liddell K, 'International Transfers of Health Data between the EU and USA: A Sector-Specific Approach for the USA to Ensure an "Adequate" Level of Protection' (2020) 7 Journal of Law and the Biosciences.
[99] DPDPA, s 16(2)

degrees of protection on transfer of personal data outside India are still applicable. The DPDPA, here, is silent on cross-border transfers aside from enabling it: the Act does not require for a standard of protection to be sought for, nor does it provide for any tests to be conducted to assess the protection of data.

Here, the GDPR far outshines the DPDPA. Despite being extremely stringent, the standard of protection and privacy that it strives for does indeed work toward achieving protection of personal data, which the DPDPA is lacking on.

While the enabling of cross-border transfer of data by a blacklisting system is applauded as a progressive move that greatly simplifies such transfers, it is suggested that transfer of data to different countries are preceded by checks and tests which assess the protection levels of data. Simply transferring a patient's data to another country without assessment of its protection would inevitably result in breach of the data and would be severely detrimental to the privacy of the individual. Medical data of a person is extremely personal and sensitive, and as such, it must be ensured that medical data and transfer of data in the healthcare industry to different countries is protected by appropriate safeguards. It is recommended that privacy of health data be given the utmost importance and safeguards on such cross-border transfer of data be implemented immediately.

CONCLUSION

Data in today's world is incredibly vast and this trait extends itself to health and medical data; hence, the sheer quantity of information exchanged is so high that it is impossible to regulate all data with 100% efficiency. As a result of this, it becomes essential to ensure adequate regulations for Data Privacy and Protection. Throughout this Study, the issues of Categorization of Health Data, De-Identification of Personal Data, Definition of Reasonable Security, and the scope for Cross-Border Transfer of Health Data have been examined in light of India's latest DPDPA.

In essence, the Study has concluded with several suggestions for each of the individual issues that have been examined in the study. The Study

ultimately concludes with the need for advancement of Privacy legislations in the Healthcare Industry. Due to the high risks associated with such data, it is necessary for the Central Government to implement subsequent sector specific regulations to effectively address the several issues concerning Data Privacy in the Healthcare Sector.

Through the Analysis of several international jurisdictions, the Study has concluded the need for more defined categorization and classification of health data to enable smooth and effective obligations that are necessary for such data of high severity. Furthermore, the Study has also identified the need for effective regulations concerning De-Identification of Data for the purpose of Research and Development. Implementing guidelines and regulations concerning de-identification in the healthcare industry will allow organizations to effectively ensure appropriate de-identification methods catered to protecting the rights of individuals. Moreover, the Study has also suggested for redefining the scope of reasonable security under the DPDPA by providing certain requirements for the healthcare industry so as to reduce the ambiguity of what constitutes a reasonable safeguard. Finally, the study suggests for the amendment of Cross-Border Regulations under the DPDPA to adopt a GDPR-like framework, encompassing privacy protection, security, and sector-specific rules for healthcare data.

While it is undeniable that the DPDPA is still at a nascent stage, it is necessary for the Central Government to introduce amendments and sectoral regulations to better suit all industries and sectors that would benefit from additional regulations, such as the Healthcare Sector. The ambiguity in the DPDPA could potentially result in dangers to the Rights of Individuals and hence, the suggestions made in this Study, would be a welcome change for the protection of data.

DISCLAIMER

This study has been conducted on the available Primary and Secondary sources for which the authors are exclusively responsible for this original work. There is no conflict of interest in the study presented by the authors.