A STUDY ON THE PERSONAL DATA PROTECTION BILL IN INDIA

Under the Guidance of:

Dr. Dhirendra Kumar

Submitted By:

Akanksha Sharma

MBA Health Management

Roll No. 1243

INTRODUCTION:

‘Digital India’ has enhanced the lives of Indians using technology. India is among the highest consumers and producer of data per capita in the world. The ABDM (Ayushman Bharat Digital Mission) is a project of Government of India that aims to digitize the health ecosystem of the country by creating digital medical records and registries for healthcare professionals and healthcare facilities.

Therefore, for the protection of data principal’s personal data across the National Digital Health Ecosystem, a comprehensive health data management policy framework must be issued. The digital protection bill must frame out the rights of citizens as well as their obligations which must be followed when the personal data is being used by the data fiduciary.

- ABDM has led to the creation of 34,80,13,866 ABHA (Ayushman Bharat Health account) creation since its inception in 2021. The mission is accelerating with the creation of approximately 5.5 lakh ABHA Id and 7.9 lakh health account linked daily according to the trend in last month. Also, platforms such as Digilocker and Aadhar generation (1,365,692,961 Aadhar have been generated till date) have boosted the creation of a digital ecosystem. Such a massive digital ecosystem also increases the vulnerability to data breaches.
- The sensitive health data of patients is very prone to data breaches in the absence of strong legal regulation. In recent years, the health records of the patients have been leaked online. Health records of more than sixty-eight lakh patients and doctors were hacked from a healthcare website in India in 2019. Also, in 2021, COVID-19 lab results of more than 1500 Indian citizens were leaked online from the government websites. Records of more than 200,000 patients were leaked from a multispecialty hospital in Kerala in 2021.

- The reasons for increased cyber-crimes in India are manifold including the following:

❖**Lack of cyber security awareness:** There are several Indians who do not realize the potential risks that their use of the internet may pose and fail to take any appropriate safeguard measures for data and devices.

❖**Poor cyber security infrastructure:** Despite the government's efforts to improve cyber security infrastructure, many organizations in India still have inadequate security measures in place, making them vulnerable to cyber-attacks.

❖**Increased adoption of technology:** As more people use online services and digital gadgets, there are more opportunities for cybercriminals to carry out their nefarious operations.

- **Inadequate legal infrastructure:** India's legal framework for cybercrime is still being developed, and as a result, there are many inconsistencies that make it difficult to convict those who commit cybercrimes.
- **Poor execution:** When dealing with reported cybercrimes, law enforcement organizations might encounter difficulties due to limited resources or insufficient expertise necessary to carry out comprehensive investigations and guarantee the prosecution of perpetrators. This leads to inadequate enforcement measures being taken.
- **Cybercriminals operating beyond India's borders:** A range of cybercriminals are active outside of India, posing challenges for law enforcement agencies in identifying and apprehending them.

Difference between 2019 PDPB and 2022 PDPB		
PDPB	2019 Draft	2022 Draft
Scope and applicability	Processing of personal data by organizations both within India and outside by organizations that offer goods or services to individuals in India or that process personal data in India.	Personal data processed online within India
Lawful processing	Includes Consent, Public interest, legal obligation.	Consent and Deemed Consent
Consent	Clear, specific, informed, and capable of withdrawal	Explicit consent and deemed consent. Explicit consent refers to a clear and specific consent given by an individual for a particular processing activity. Deemed consent is a term used to describe the situation in which an individual's permission can be assumed or implied.
Registration	Data Fiduciaries	Consent Manager

Appointment of DPO	**Mandatory for data fiduciaries. Based in India**	**Mandatory for data fiduciaries.**
Breach Notification	Data fiduciary to Data Protection Authority	Data Fiduciary/Processor to Data Protection Board
Data Principal's Rights	The person who owns the data has the right to access their personal information, correct any errors, and exercise the right to data portability.	The individual whose data is being referred to has the ability to designate and holds the right to correct their personal information, obtain details about it, and seek resolution for any complaints.
Penalty	Fine up to 15 crore or 4% of global turnover and imprisonment up to 3 years.	Fine to data principal up to 10,000 and to data fiduciary up to 500 crores for each instance.
Transfer of data cross border	The transfer of personal data is permitted only if the consent for such transfer has been given by the data principal and such transfer has been approved by the data protection	List of countries to which personal data can be transferred will be provided by Central Government

LITERATURE REVIEW:

Author (Year)	Study Location	Sampling Technique	Salient Features
N Terry. 'Existential challenges for healthcare data protection in the United States' (2017)	USA	Descriptive	HIPAA has limited scope in its application. It is specific to domains and offers protection primarily in downstream contexts. The challenges include the data which lies outside traditional healthcare system
Dona Budi Kharisma and Alvalarie Diakenza. 'Patient personal data protection: comparing the health-care regulations' (2022)	Indonesia, EU, Singapore	Descriptive	There is currently no legislation in Indonesia pertaining to personal data protection. Singapore and the European Union (EU) experience fewer instances of patient personal data breaches due to their regulatory frameworks that particularly address the security of such data.

Author(Year)	Study Location	Sample Size	Sampling Technique	Salient Features
Hui Na Chua et.al. 'Compliance to personal data protection principles: A study of how organizations frame privacy policy notices' (2017)	Malaysia	306	Convenient Sampling	Private organizations have more adherence to the PDPA (Personal Data Protection Act) requirements as compared to public organizations and non- governmental organizations have more compliance as compared to governmental organizations.
Al Sentot Sudarwanto et.al. 'Comparative study of personal data protection regulations' (2021)	Indonesia, Hong Kong, Malaysia		Descriptive	In terms of value, Indonesia possesses the largest digital economy in South Asia; however, data breaches pose a significant challenge. There is currently no regulation or commission in place in Indonesia specifically dedicated to the protection of personal data. Furthermore, there are no existing regulations pertaining to criminal sanctions or civil claims related to data breaches.

RESEARCH QUESTION & METHODOLOGY:

- **Research Question:** What are the characteristics of an effective Personal Data Protection Bill in India?
- **Objectives:**

❖General objective: To determine the characteristics of Personal Data Protection Bill in India to protect patients' health data from all over the country.

❖Specific Objectives:

➢To analyze the best practices regarding data protection bill in countries of USA, UK, Singapore, and Malaysia to understand the characteristics such as accountability & enforcement mechanisms, data transfer mechanism, data retention mechanism, consent for collecting data.

➢To analyze the data protection policies put in place by the Indian Government to protect consumers' personal data.

- **Research Design** – Descriptive cross- sectional study.
- **Study Setting** – India

❖Study Population – Bureaucrats, Policy makers

➢Inclusion Criteria: Data protection bills of USA, UK, Singapore, and Malaysia.

➢Exclusion Criteria: Data protection bills of other countries

❖Study Tools: Questionnaires for conducting interviews and review of data protection bills of the above-mentioned countries.

- Duration of Study: 3 months from March 2023 to May 2023
- Sampling Technique: Convenience Sampling
- Data Collection Procedure: Semi structured Interviews and review of records.

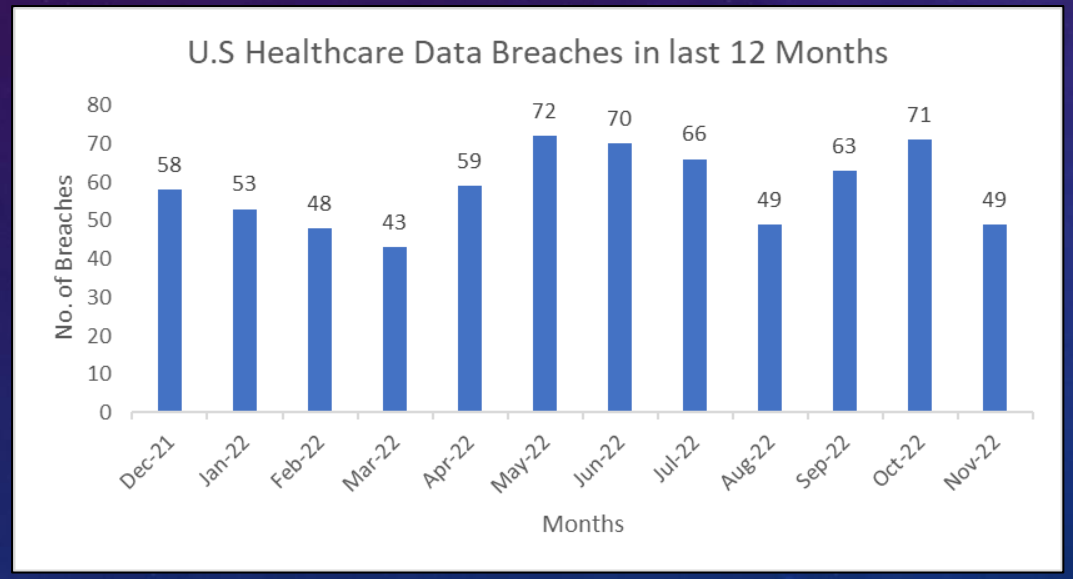
RESULTS:

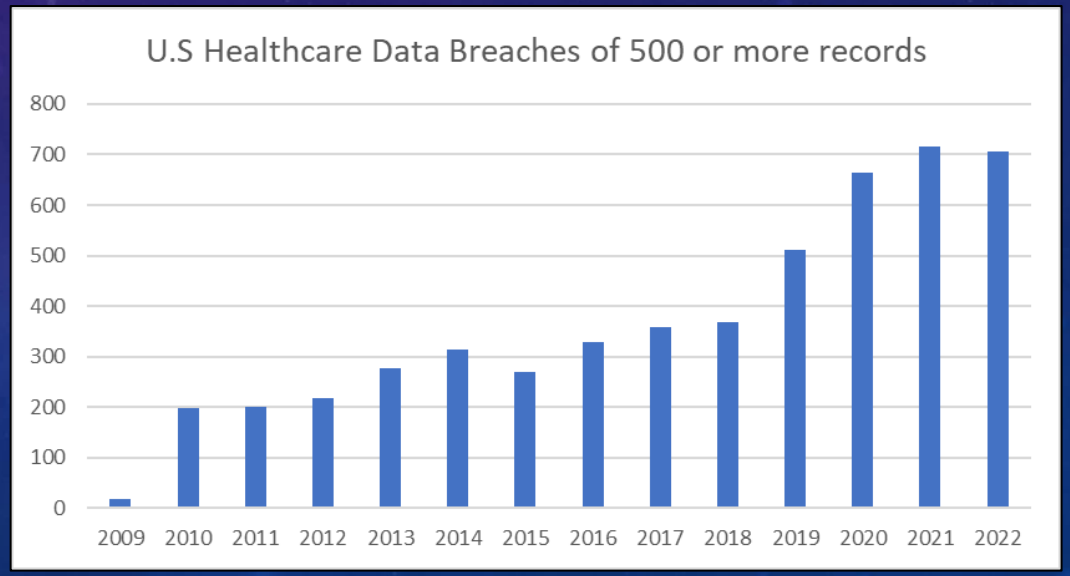
- **USA:**

❖HIPAA, the Health Insurance Portability and Accountability Act, is a law specifically designed to protect healthcare data. It protects personal information of the patient from being made public in a manner that is unauthorized.

❖To enforce the Privacy Regulations outlined by the Health Insurance Portability and Accountability Act (HIPAA), the US Department of Health and Human Services (HHS) introduced the HIPAA Privacy Rule.

The Privacy Rule establishes comprehensive regulations on a national level to protect the privacy and confidentiality of individuals' medical records and other sensitive health information (PHI).It is applicable to health plans, healthcare clearinghouses, and healthcare providers that electronically transmit health information. The Privacy Rule provides patients with important rights to access and manage their personal health information (PHI) while imposing restrictions on the utilization and sharing of PHI by entities subject to the rule.





Characteristics of Health data protection bill across countries					
Characteristics	**USA**	**UK**	**Singapore**	**Malaysia**	**India Draft Bill 2022**
Primary law	HIPAA	Data Protection Act 2018	Singapore Personal Data Privacy Act	Malaysia Data Protection Act	None
Regulatory Body	US Department of Health and Human Services.	Information Commissioner Officer	Singapore Data Protection Authority	Personal Data Protection Department	Data Protection Board
Applicability	Entities subject to regulation, such as healthcare providers, health plans, and healthcare clearinghouses.	Health data, including by healthcare providers and other data controllers	Health data, including by data users	Health data, including by data users	Health data, including by data fiduciaries
Additional Health-Related Legislation	n/a	Health and Social Care Act 2012	n/a	n/a	n/a

Characteristics	USA	UK	Singapore	Malaysia	India Draft Bill 2022
Data Processing	Governs the utilization and sharing of PHI (Personal Health Information).	Oversees the utilization and dissemination of personal data, including health-related information.	Controls the handling of personal data, encompassing health-related information	Manages the gathering, utilization, and sharing of personal data, encompassing health-related information	Controls and governs the handling of personal data, including health-related information
Rights for Individuals	Provides patients with the authority to access and manage their PHI (Personal Health Information).	Provides individuals with specific rights concerning their data, including the privilege to access and correct their information.	Provides individuals with specific rights concerning their data, including the privilege to access and correct their information	Provides individuals with specific rights concerning their data, including the privilege to access and correct their information	Grants individuals' certain entitlements regarding their data, which include the right to access, correct, and erase their personal information.
Max.Penalty	$1.5million.	€20 million	SGD 200,000	MYR 300,000	INR 500 Cr.

Thematic analysis of qualitative data		
Themes	**Description**	**Examples from Interviews**
Health data collection & usage	Collection and usage of health data by organizations.	“Organizations should follow proper guidelines for the collection of health data from the individuals.”
Health Data privacy	Privacy of individuals personal data.	“Privacy should be maintained in case of data that is being collected from the individuals”
Health Data Security	Measures to secure the security of health data, preventing illegitimate access.	“Health data collected should be protected from unauthorized access in order to ensure the safety of the individuals.”
Accountability	Organizations accountable for violation of law.	“Heavy penalties should be imposed on organizations from which the sensitive health data is leaked”
Application of health data in research	Utilization of individual health data for research objectives.	“Organizations that want to use the personal data for the research should obtain informed consent from the individuals”.

Themes	Description	Examples from Interviews
Grievance redressal	Appropriate grievance redressal mechanisms for the individuals.	“There is a grievance redressal mechanism in the draft bill through which the individuals can file complaints with the DPA”
Cross border transfer of data	Transfer of health data across National borders.	“There should be proper guidelines for the cross-border transfer of health data to protect the sensitive information of the patients.”
Regulatory body	The suitable regulatory authority tasked with overseeing the execution of the Personal Data Protection Bill in India.	“There should be a regulatory body to oversee that the bill is implemented in the country”.

DISCUSSION:

- Drawing upon global best practices and insights from interviews with policy makers, it can be determined that the data protection bill in India should be all-encompassing, with special emphasis on safeguarding healthcare data of individuals. The bill must have strong provisions to guarantee the protection of individuals' personal information. It should include the following characteristics:

❖Precise and inclusive terminology: It is necessary for the law to offer clear and comprehensive explanations of key terms and principles such as "personal data," "sensitive data," "processing," "consent," "data controller," and "data processor." By doing so, the legislation guarantees that its extent and applicability are easily understood and consistent for everyone involved.

- Robust data protection principles: The legislation should encapsulate robust principles of data protection, including data minimization, purpose limitation, accuracy, transparency, and security. These principles guarantee the fair and lawful collection, processing, and utilization of personal data while implementing adequate measures to safeguard against unauthorized access, use, and disclosure.
- Transparent and easily exercised rights for individuals: The law should offer clear and easily comprehensible entitlements for individuals, encompassing the entitlements to access, correct, delete, and restrict the processing of their personal data. These rights should be readily accessible, user-friendly, and enforceable through effective legal remedies.

- Measures for accountability and enforcement: The legislation should introduce mechanisms to promote accountability and enforce compliance, thereby ensuring that data controllers and processors are held accountable for adhering to the law. It is crucial to have effective sanctions in place for instances of non-compliance.
- International data transfers: The legislation ought to establish unambiguous guidelines regarding the transfer of personal data to countries beyond its jurisdiction, while also guaranteeing the implementation of sufficient measures to safeguard the data.
- Autonomous supervision: The legislation should institute a separate governing body or committee for data protection, responsible for overseeing the execution and enforcement of the law. Additionally, this body should offer guidance and assistance to data controllers, processors, and data subjects.

- Proactive measures to promote data protection: The bill should include measures to promote data protection, such as public education campaigns, privacy impact assessments, and data protection by design and by default.

With these features incorporated in the personal data protection bill, India can have an effective bill which protects the right of the individuals as well as their health information n lieu of the digital health ecosystem the Government of India is trying to create.

CONCLUSION & RECOMMENDATION:

- ABDM holds the capacity to revolutionize the healthcare industry in India through the utilization of digital technologies, enhancing the accessibility, quality, and efficiency of healthcare services. It has numerous benefits including Improved healthcare access, Enhanced patient experience, Increased efficiency and cost-effectiveness, better health outcomes and Strengthened healthcare infrastructure.
- Although it has numerous benefits, the use of digital technology also endangers the health information to various cyber-attacks. Recent years have witnessed an increased number of attacks on healthcare data. To protect the healthcare data from the cyber-crimes, India needs a robust personal data protection bill that protects the rights of the people as well as increase the trust of the people in the digital ecosystem.

The data protection bill can be implemented taking into consideration the best practices around the world. The bill should have strong rights for the data principals as well as strong accountability and enforcement mechanisms.

THANK YOU