A STUDY ON THE PERSONAL DATA PROTECTION BILL IN INDIA

Dissertation Submitted to

The IIHMR University, Jaipur

For the partial fulfillment for the award of the degree of

Master of Business Administration (MBA)

In

Hospital and Health Management

By

Akanksha Sharma

Under the Supervision and Guidance of

Dr. Dhirendra Kumar

2023

A STUDY ON THE PERSONAL DATA PROTECTION BILL IN INDIA

Dissertation Submitted to

The IIHMR University, Jaipur

For the partial fulfillment for the award of the degree of

Master of Business Administration (MBA)

By

Akanksha Sharma

Under the Supervision and Guidance of

Dr. Dhirendra Kumar

2023

DECLARATION BY STUDENT

I hereby declare that this dissertation titled “A Study on the Personal Data Protection Bill in India” is a Bonafide record of my original research work. I declare that it has not been submitted to any other institution or University for the award of any degree or diploma. Information derived from the published or unpublished work of others has been given due acknowledgement in the text.

Name of the student: Akanksha Sharma

Date: 20/05/2023

CERTIFICATE

This is to certify that Akanksha Sharma in partial fulfillment of the requirements for the award of the degree of MBA (Hospital and Health Management) from the IIHMR University, Jaipur has successfully completed her internship at Enira Consulting Private Limited during February 20-May 19, 2023.

Place: Bhavnagar

Director

Date: 20/05/2023

Enira Consulting Private Limited

CERTIFICATE

This is to certify that dissertation titled "A Study on the personal data protection bill in India" is a record of the research work undertaken by Akanksha Sharma in partial fulfillment of the requirements for the award of the degree of MBA Hospital and Health Management from the IIHMR University, Jaipur under my guidance and supervision and his/her approach to the research study has been sincere, scientific, and analytical.

Faculty Guide: Dr. Dhirendra Kumar	School Dean: Dr. (Col) Mahendra Kumar
IIHMR University, Jaipur	IIHMR University, Jaipur
Date:	Date:

Abstract:

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. Such a digital health ecosystem along with a vast number of HealthTech startups in the country increase the vulnerability of the sensitive health data to cyber-crimes. 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 the rights of citizens as well as their obligations which must be followed when the personal data is being used by the data fiduciary. The current study lays down the characteristics of an effective personal data protection for India taking into consideration some of the best practices around the world as well the interviews which were conducted for the better understanding of the bill which is currently being drafted in the country.

The draft bill to protect individuals' personal data has been drawn up by India. The Parliament has not adopted this bill and there is still scope for recommendations and amendments.

An effective personal data protection bill should have strong definitions for the data as well as accountability and enforcement mechanisms to decrease the threat of cyber-crimes and data breaches on the sensitive healthcare data.

Keywords: ABDM, Personal data protection bill, Cyber-crimes, Data Principal, policy makers

Acknowledgement:

I would like to take this opportunity to express my deepest gratitude and appreciation to all the individuals and entities who have played a significant role in the completion of my dissertation. Their unwavering support, guidance, and blessings have been invaluable throughout this remarkable journey.

I am profoundly grateful to my esteemed professors at IIHMR University for their profound knowledge, wisdom, and relentless support. Their extensive expertise and guidance have significantly contributed to shaping my research and expanding my understanding of the subject matter.

A special word of appreciation goes to my faculty guide, Dr. Dhirendra Kumar, whose exceptional guidance, patience, and scholarly insights have been instrumental in the successful completion of this dissertation. His mentorship has not only honed my research skills but also instilled in me a deep passion for academic excellence.

I would like to express my sincere gratitude to Dr. Sabine Kapasi, the Director at Enira Consulting Private Limited, for her invaluable support and guidance throughout this research endeavor. Her unwavering belief in my abilities, constructive feedback, and industry insights have played a pivotal role in shaping the direction and outcomes of my dissertation.

I would also like to extend my heartfelt thanks to my batchmates, whose constant support, collaborative spirit, and stimulating discussions have been an immense source of motivation and growth. Their camaraderie and shared experiences have made this journey more enriching and memorable.

To my parents, I owe an immeasurable debt of gratitude for their unconditional love, unwavering support, and endless encouragement throughout my academic pursuits. Their sacrifices and belief in my potential have been my constant driving force, and I am forever grateful for their presence in my life. Lastly, I would like to acknowledge the divine blessings and guidance of God. It is through His grace that I have been able to overcome challenges, seek knowledge, and find inspiration at every step of this journey.

Table of Content:

List of Figures:

List of Tables:

Abbreviations:

- PDPB – Personal Data Protection Bill
- EU – European Union
- ABHA – Ayushman Bharat Health account
- ABDM – Ayushman Bharat Digital Mission
- JPC – Joint Parliamentary Committee
- MeiTY – Ministry of Electronics and Information Technology
- DPO – Data Protection Officer
- OB – Open Bullet
- IoT – Internet of things
- DPA – Data Protection Authority
- HIPAA – Health Information Portability and Accountability act
- FCRA – Fair credit reporting act
- FERPA – Family Educational Rights and Privacy act
- GLBA – Gramm-Leach-Bliley Act
- ECPA – Electronic Communications Privacy act
- COPPA – Children's Online Privacy Protection Rule
- VPPA – Video Privacy Protection Act

Chapter 1: 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. There are various instances of data breach in the country owing to the absence of any regulatory framework hence a legal framework must be established taking into consideration some of the existing regulations regarding the same in countries such as USA, UK, Singapore, and Malaysia.

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. In addition, there are 7849 Health Tech startups in India. (6) These also increase the vulnerability to cyber crimes

To address these challenges, Government of India had started the work to a draft personal data protection bill in 2017, but the bill still has not been passed by the Parliament. The digital protection bill draft in India has undergone through various changes since its inception. The timeline of the evolution of data protection bill in India is as follows:

August 2017- Supreme court recognizes privacy as fundamental right. → A 10-member committee formed which submitted report in 2018. → Draft bill formed by MeiTY in 2019 suggested that personal data can be processed only for a clearly defined purpose and users should be given the choice to withdraw consent. It was suggested that personal data of individual must be processed only on local servers and all firms should hire a data protection officer.

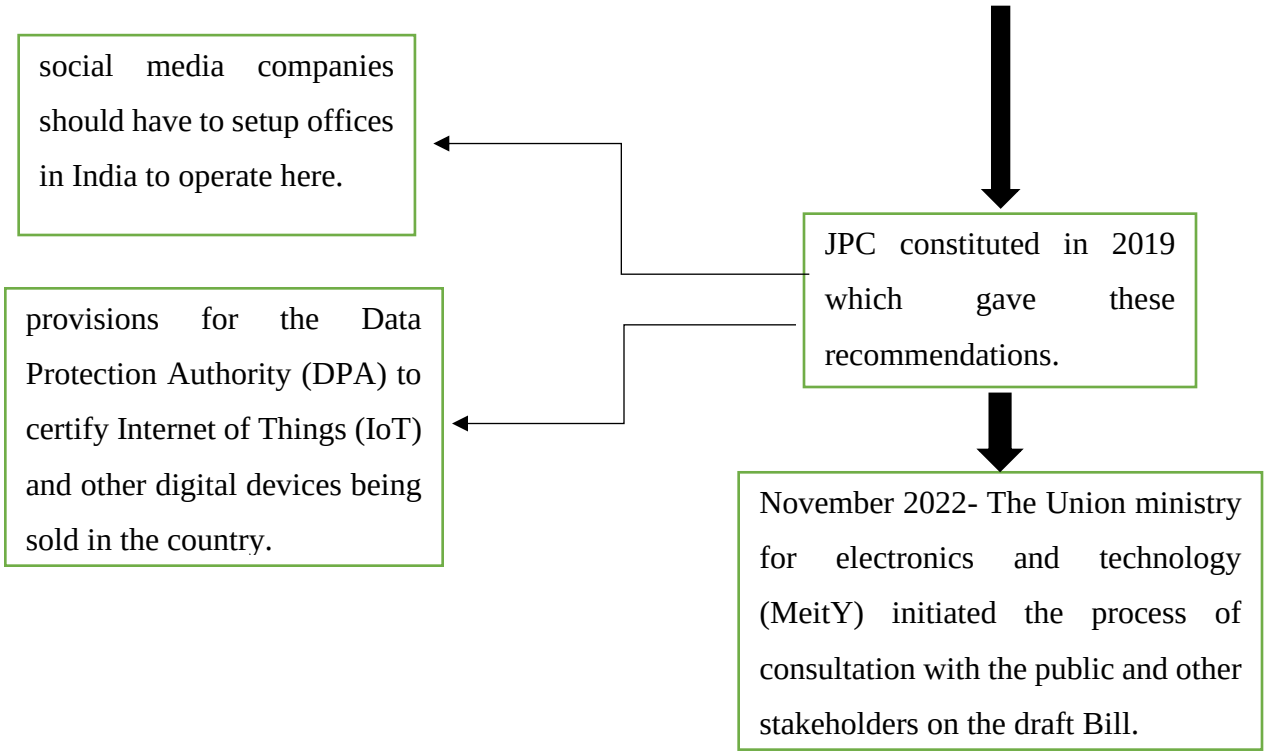

Figure1.1 – Timeline of data protection bill in India

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. (1) 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. (2) The occurrence of sensitive data breaches emphasizes the need for well-functioning data protection legislation within the nation. The United States has been identified as the most targeted country in terms of attack on healthcare data with 32.1% of the worldwide attacks on healthcare industry being done in USA and India, China and Italy were the second most targeted country for healthcare data attacks each having 7.7% of total healthcare attacks in 2021. In 2021, COVID-19 vaccination records of 150 million were sold online by the hackers Also, in August 2021, OB(OpenBullet) configurations to online pharmacy Net meds were shared for free by the hackers which compromised the accounts of the users. In July 2021, 289,000 records from Dental Workers USA (online staff recruitment platform for dentists) and 55,960 records from Desi Zip India (online classified website for businesses, products & services) were leaked online. (3)

These instances have been on the rise and there is a need to create legislation that protects the personal data of the users. A digital health management policy with a citizen centric approach must be developed to ensure that the citizens have an agency which can inform them regarding their choices, to have them exercise their rights and which helps solve their grievances. Therefore, a data protection bill must be enacted considering the various best practices around the world on similar subject and how it is possible to implement these practices in the Indian context. The countries in which these practices are followed include those of USA which have HIPAA, UK, Singapore, and Malaysia.

Cyber-crimes have increased manifold in recent years. Globally, they increased to 125% in the year 2021. The most common type of crime online includes phishing with around 323,973 internet users affected in 2021. The UK had the highest number of cyber-crimes in 2022, with 4783 people falling victim to cybercrime for every million internet users, while the United States represented 1494 victims. (4) In India, the cyber-attacks increased from 41378 in 2017 to 1402809 in 2021 according to a report by the CERT-In. (5) Highest cyber-crimes were reported from the state of Telangana in the year 2021 with 10,303 cases. (20)

The costs of data breaches vary from one country to another based on gross domestic product, level of technology employed and national data protection laws. (29)

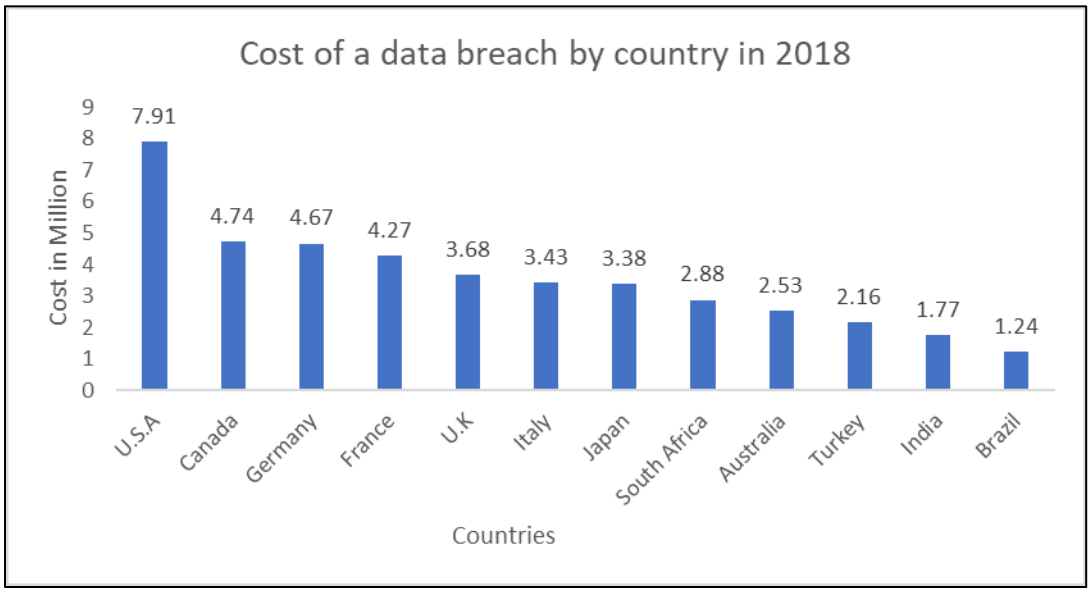

Figure 1.2 Cost of a data breach by country in 2018

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.

In general, it is crucial for individuals and organizations in India to recognize the significance of cyber security and respond accordingly to safeguard themselves against cyber threats. It is essential for the government to consistently enhance the legal structure and enforcement mechanisms concerning cyber-crimes. To address these problems, the Government has developed a draft Law called “Digital Personal Data Protection Bill” in 2022, which differs substantially from its predecessor enacted in 2019, and is intended to deal with these issues.

The primary distinction between the 2022 draft bill and the 2019 bill is that the former excludes non-sensitive personal data, whereas the latter encompasses such data. Furthermore, the 2022 legislation does not cover nonautomated processing of personal data or personal data used by individuals for personal purposes, which were included in the 2019 legislation. Personal data that were included in the 2019 bill as personal data (Personally identifiable information), sensitive

personal data (highly sensitive personal information), critical personal data (crucial personal information) are also not classified in the bill. This bill considers all personal data at par irrespective of its sensitivity.

Table 1.1 Difference between 2019 PDPB and 2022 PDPB		
PDPB	**2019**	**2022**
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 fifteen 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 five hundred 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 authority.	List of countries to which personal data can be transferred will be provided by Central Government.

However, these recommendations are still under consideration before the bill is tabled in parliament. The need for the data protection regulation in India is urgent as digitization is being encouraged in the country at a very vast level in all the sectors including the healthcare. Health data is highly vulnerable to data breach as it contains sensitive information about the individual including the medical conditions. Hence, to protect the individual data and to encourage the trust of the people in the digital health ecosystem that is being created in the country, it is required that the personal data of the people be protected.

Chapter 2: Review of Literature:

Author (Year)	Study Location	Sample Size	Sampling Technique	Salient Features
N Terry. 'Existential challenges for healthcare data protection in the United States' (2017) (8)	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 et. al. 'Patient personal data protection: comparing the health-care regulations' (2022) (9)	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.
Dimitra Georgiou et.al. 'Compatibility of a Security Policy for a Cloud-Based Healthcare System with Data Protection Regulation' (2020) (16)	European Union		Descriptive	Security challenges associated with complying with GDPR when adopting cloud technology in healthcare may impede the process of transferring healthcare systems and data to cloud-based platforms. Security challenges include Data Reliability, Data Management,

				Cloud Security, and Data Breach. Rules that the organizations and providers that operate in the cloud should follow.to manage the data subject's request include: Gathering the inquiry made by an individual regarding their personal data; Verifying the identity and gathering relevant details or particulars regarding an individual's data to process the request; Registration of the request in the requests' record; Forwarding the request to the data protection officer; Assessing the request; Requesting further information from the individual if necessary; notifying the data subject of any applicable fees associated with processing the request; Performing the required actions; Providing valid reasons to the individual for the delay in fulfilling their solicitation; Informing the DPO regarding the implementation; Prepare the response document for the individual; Updating the individual about the status of

				their solicitation, whether it has been fulfilled or not.
Angelo Costa et.al. 'A legal framework for an elderly healthcare platform' (2017) (10)	Portugal		Descriptive	The concept of Ambient Assisted Living (AAL) offers cost-effective technological solutions that enable the provision of medical assistance through devices and services. Privacy in the AAL applications is a concern. AAL applications gather sensitive patient data, and both Article 17 of the Data Protection Directive and Article 32 of the GDPR establish requirements for ensuring data security. These requirements emphasize the need for implementing suitable technological and operational actions taken to hinder unauthorized or illegal handling of personal data, maintain data confidentiality, and safeguard against accidental or unlawful occurrence of personal data being lost, harmed, or annihilated
Teodora Lalova-Spinks et.al.	European Union	191	Convenient sampling	The primary obstacle in healthcare research pertains to the lack of legal harmonization.

'Challenges related to data protection in clinical research before and during the COVID-19 pandemic' (2022) (17)			using online survey	The challenges associated with delivering information to patients were intensified because of crisis measures implemented worldwide.
S Trent Rosenbloom et.al. 'Updating HIPAA for the electronic medical record era' (2019) (31)	USA		Descriptive	One of the challenges faced by HIPAA is the absence of federal regulations specifically addressing software companies that utilize consumer technologies to handle personally identifiable health information. Furthermore, HIPAA's right to access does not encompass non-covered entities (NCEs) that collect similar data. In 2019, the Office of the National Coordinator for Health Information Technology (ONC) introduced new policies, including a revised definition of EHI (Electronic Health Information). This updated definition includes information that can be shared directly by individuals themselves or through technology chosen by individuals, with entities covered by information blocking provisions.

Hui Na Chua et.al. 'Compliance to personal data protection principles: A study of how organizations frame privacy policy notices' (2017) (32)	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) (33)	Malaysia, Indonesia, and Hong Kong		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.
Shruti Kesarwani. Public Perception of the Personal Data Protection Bill (2021)	Pune, India	25	Qualitative Research	Explores the public's perception of the Personal Data Protection Bill through semi-structured interviews with 25 participants. The study found that most participants were concerned about the lack of transparency in data processing and the potential

				misuse of personal data by companies.

Chapter 3: 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.

Data Analysis Plan**:** Thematic analysis was done on the data collected from the interviews analysis as it is a commonly used method for analysis of qualitative data. In addition, Data protection bills of the above-mentioned countries was reviewed to study the best practices which can be incorporated in the data protection of India to develop a comprehensive bill for protection of personal as well as health data of the people of India.

The operational definitions used in the study are as follows:(10)

- Data – Data is representations of information, facts, and concepts capable of being communicated, interpreted, or processed in a manner that is acceptable to humans or by electronic means.
- Data Principal – The person to whom the personal data is related. As regards children, parents or legal guardians are to be considered as data principal.
- Personal Data – Any data by which or in relation to which an individual can be identified.
- Data Fiduciary – The entity which decides the means of processing the individual's personal data. It can be firm, individual, or state.
- Processing – It refers to the entire operations associated with personal information.
- Safeguarding of data - Data protection can be defined as a collection of practices, policies, and procedures implemented to safeguard personal data, prevent unauthorized access, use, disclosure, or destruction.
- Data Ownership – It refers to the legal right of an individual or organization to claim the ownership of a particular set of data.

Ethical Considerations –

- For the policy documents, the data available in the public domain was used hence the risk of revealing or sharing the personal information of the individual in question is prevented.
- To conduct interviews, informed consent was obtained from the participants.

Chapter 4: Results

The best practices in the protection of healthcare data around the world include the various data protection regulations in the following countries:

USA:

USA has various laws for data protection in the country namely HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA. 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 the disclosure or sharing of protected health information (PHI) by entities that are obligated to follow the rule. The covered entities under the privacy rule include:

Table 4.1 HIPAA Rule Covered Entities

Healthcare Practitioners	Health Plan	Health data aggregators	Service providers
Physicians, care providers, psychologists, dentists, chiropractors, nursing houses and pharmacies are all types of providers, but they	It includes: Insurance coverage for medical, dental, vision, and prescription drugs, as well as health maintenance	These are those entities which, in turn, process the invalid information received from another entity into a	The person or organization that uses identifiable health information to carry out certain operations or fulfil functions of a covered entity shall be included. The

shall be required to provide health information by means of electronic transmission in connection with the covered transactions. The covered transactions involve the transmission of healthcare information for payments, medical operations and some other activities relating to health care provision. Health insurance companies and health information exchange providers that transmit healthcare data electronically for covered transactions shall also be subject to the Privacy Rule.	organizations (HMOs). Medigap, Medicaid, Medicare + Choice, and Medigap supplement insurance. Insurers that provide coverage for extended care (excluding fixed-indemnity policies for nursing home care). Healthcare plans provided by employers for groups of individuals. Healthcare plans supported by government entities and religious institutions. Healthcare plans catering to multiple employers.	standard format or vice versa.	processing of claims, data analysis, utilization review and billing may be part of these activities.

According to the HIPAA Journal (28), there have been various data breaches in healthcare in the last 12 months and the number of healthcare data breaches of five hundred records or more have been increasing since 2009. They include:

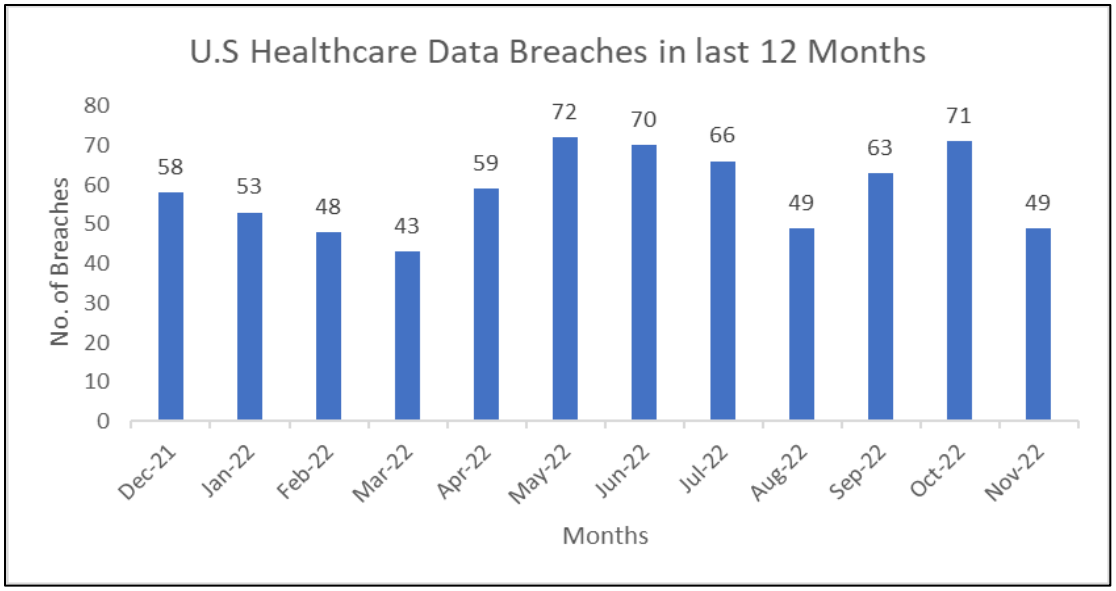

Figure 4.1 US Healthcare Data Breaches in last 12 months

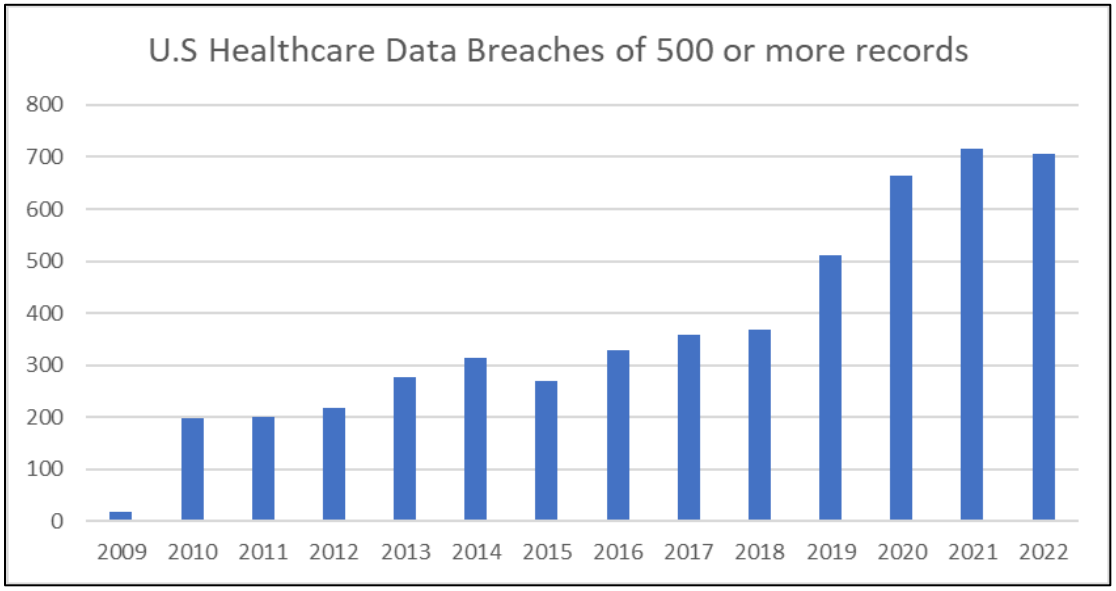

Figure 4.2 US Healthcare Data Breaches of five hundred or more records.

The regulation on privacy allows for the sharing of Health records of patients or individuals' medical information without obtaining the patient's consent for the following intentions:

1. Mandatory Legal Obligation: Covered entities are authorized to disclose PHI when compelled by legal requirements, such as complying with a court order or responding to a subpoena.
2. Public Health Initiatives: Entities subject to regulation are permitted to reveal Patient Health Information (PHI) for the purpose of public health activities, which involve actions such as reporting contagious diseases, monitoring vital statistics (births and deaths), and carrying out investigations related to public health.
3. Individuals who have experienced abuse or domestic violence.
4. Supervision of Healthcare Operations: Covered entities have the authority to disclose PHI to health oversight agencies, even without the patient's authorization, for activities like audits, investigations, and inspections related to ensuring the quality and compliance of healthcare operations.
5. Legal and Administrative Proceedings: Entities subject to regulation are authorized to disclose Patient Health Information (PHI) in accordance with a court order, subpoena, or any other legally mandated process in judicial or administrative proceedings.
6. Law enforcement
7. Responsibilities Regarding Deceased Individuals: Covered entities have the authority to disclose PHI for purposes concerning deceased individuals, including tasks such as identifying the deceased person, determining the cause of death, and arranging for the proper handling of the body.
8. Assisting Organ, Eye, or Tissue Donation and Transplantation: Patient Health Information (PHI) can be shared to facilitate and facilitate the procedure of eye, organ, or tissue donation and transplantation.
9. Research with Specific Conditions: Covered entities have the option to disclose PHI for research purposes, but with specific conditions in place. These conditions may include obtaining approval from an institutional review board (IRB) or acquiring a waiver of authorization.

10. Disclosing PHI to Prevent Serious and Immediate Harm: PHI can be shared in cases where there is a clear and immediate potential danger to the well-being or safety of an individual or the public, aiming to prevent harm.
11. Vital Government Operations: Covered entities have the authority to disclose PHI for crucial government functions, which may include activities related to national security and intelligence.
12. Occupational Injury or Illness Compensation: Covered entities can disclose PHI as required to fulfill obligations under workers' compensation laws and similar programs that offer benefits for injuries or illnesses related to work.

The HIPAA violation penalty structure includes both civil and criminal penalties, with the severity of the penalties varying depending on the level of culpability involved. The responsibility to enforce the privacy and security rules of HIPAA lies with the United States Department of Health and Human Services.

The following civil penalties are applicable to HIPAA infringements:

Tier 1: Unknowing infringements - The penalties for each violation range from $100 to $50,000, with a yearly cap of $25,000 for repeated violations.

Tier 2: Reasonable cause infringements - The penalties for each violation vary between $1,000 and $50,000, with an annual maximum of $100,000 for repeated violations.

Tier 3: Intentional Negligence, remedied within 30 days - Penalties vary between $10,000 and $50,000 per violation, with a yearly limit of $250,000 for recurring violations.

Tier 4: Deliberate Negligence, Not Remedied within 30 days - Penalties vary between $50,000 and $1.5 million for each instance of violation, and for recurring violations, there is an annual limit of $1.5 million.

HIPAA violations can lead to criminal penalties that involve fines and imprisonment, the severity of which depends on the nature of the offense. The penalties can range from fines of $50,000 to $250,000, coupled with imprisonment for a maximum of 10 years for deliberate or intentional violations. In cases of unauthorized access or disclosure of PHI, the penalties may include fines of $100,000 and imprisonment for up to one year.

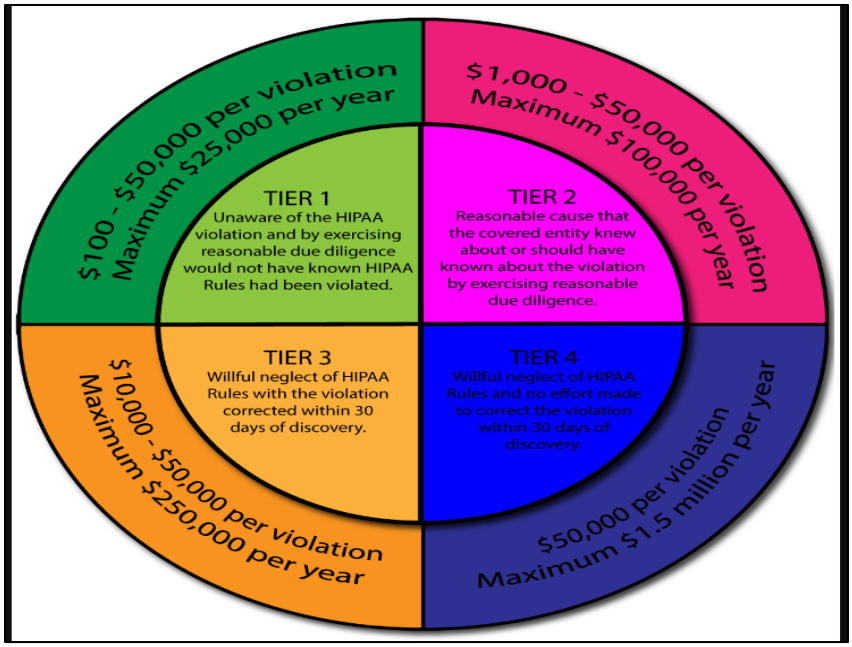

Figure 4.3: HIPAA Violations penalty structure

Source – HIPAA Journal (28)

UK:

The United Kingdom has implemented the Data Protection Act 2018 in compliance with the General Data Protection Regulation (GDPR). The purpose of this Act is to facilitate the transfer of data in a secure manner within the EU. The definition of health data in the legislation refers to "information about an individual's physical or mental well-being, including the medical services they receive, which discloses details about their health condition." The law specifies that the right to access such health data is not subject to the regulations outlined in the Data Protection Act 2018. This exemption is as follows:

- If data is utilized for the purpose of strategic forecasting or planning concerning the delivery of health or social care by a public authority, and granting access to the data could potentially hinder the attainment of those objectives.
- If disclosing the data for research purposes would pose a risk of compromising the integrity or validity of the research, access may be denied.
- If granting access to the data for statistical purposes would potentially undermine or hinder the process of preparing accurate statistics, access may be denied.

- If the data is used for the purpose of assessing eligibility for social security benefits or services and granting access to the data may potentially compromise the effective administration of those benefits or services.

The Health Research Authority (HRA) receives counsel from the CAG on applications for accessing confidential patient information for research objectives. The CAG comprises of independent professionals from fields such as law, ethics, patient advocacy, and information governance, who regularly convene to examine requests for access to such data. The recommendations made by the CAG (Confidentiality Advisory Group) are based on a set of moral guidelines and legal requirements governing the utilization of patient information in research initiatives. Their goal is to determine whether the proposed utilization serves the public interest and has enough protections for patient confidentiality. The main responsibility of the CAG is to ensure that research projects utilizing such data are carried out securely and ethically, prioritizing the privacy and confidentiality of patients. This is in addition to advising researchers on the legal and moral implications of accessing sensitive patient information.

The Information Commissioner's Office is responsible for overseeing the enforcement of data protection regulations in the UK, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The key objective for the ICO is to protect information rights, uphold data protection and preserve privacy. To do this, the ICO is empowered to investigate data protection violations, carry out audits to determine if organizations are complying with data protection rules, and impose penalties and fines for non-compliance. The ICO also provides advice and direction to people and organizations on data protection and privacy issues, covering a variety of subjects such data protection principles, consent, subject access requests, and international data transfers. The ICO has acted when data protection laws are not followed. In case of a serious data leak, which might involve violations of basic principles like transparency, lawfulness, due process, and individuals' rights to access or delete their personal health information, the General Data Protection Regulation allows for penalties of a maximum amount of EUR 20 million, or 4% of the organization's worldwide income.

Singapore:

In Singapore, the primary legislation that regulates data protection is the Personal Data Protection Act (PDPA), which offers a basic level of protection for personal data. Protecting personal data of individuals and ensuring that organizations manage such data responsibly and transparently are the main goals of the PDPA. In addition to the PDPA, there are rules and structures catered to certain industries that support its objectives. The PDPA applies to all businesses in Singapore that collect, use, or disclose personal data, regardless of industry or sector. Under the PDPA, organizations are obligated to adhere to various obligations, which entail obtaining individuals' approval prior to collecting, managing, and revealing their personal data, enabling individuals to have access to their own data and implementing robust security measures to prevent unauthorized access.

The Personal Data Protection Act (PDPA) in Singapore, Section 21(1), states that whenever a person asks access to their personal data from a company, the company must give the person a replica of their individual data. Furthermore, the organization must also provide information regarding the utilization or potential disclosure of the data by the organization. This information can include details such as the intended objective behind the data collection, the entities, or individuals with whom the data has been shared and any transfers of the data outside of Singapore. Under the Act, individuals possess the entitlement to request access to their personal data and to seek rectification of any inaccurate or incomplete personal data. Organizations are obligated to promptly address these requests and furnish the requested information in a timely manner. The provision of requested information is typically free of charge, unless the request is clearly baseless or excessively burdensome.

Failure to comply with the access and correction obligations under the PDPA can result in fines and other penalties, as well as reputational damage and loss of customer trust. The Protection Obligation requires organizations to male sufficient security arrangements to protect the data which is in their possession. This includes both physical and technological security measures, such as restricting the ability to retrieve personal data, securing personal data during transmission and storage through encryption, and regularly reviewing and testing security systems. Healthcare institutions should pay special attention to the characteristics or attributes of the personal data in their possession or control and adopt appropriate security measures to protect such data. This may

include implementing access controls, encryption, and the adoption of technical and operational safeguards to ensure the security of personal data against unauthorized access, utilization, or disclosure. According to Section 25 of the PDPA, if an organization has gathered personal data for a specific purpose, such as a particular project or transaction, and that purpose has been fulfilled or no longer exists, the organization should no longer retain the said personal data unless there is a lawful or business justification for doing so. If the personal data becomes unnecessary, the organization should dispose of it or render it anonymous to prevent it from being associated with identifiable individuals. However, there might be legal or business considerations that necessitate the retention of personal data for an extended duration. In such cases, the organization must ensure that they have a legitimate reason for retaining personal data and have implemented suitable measures to protect it against unauthorized access, use, or disclosure. The organization must promptly cease collecting, using, or disclosing personal data upon withdrawal of consent and take appropriate actions to delete or anonymize the personal sensitive data expeditiously.

Malaysia:

In Malaysia, the Personal Data Protection Act (PDPA) safeguards health data as a specific category of personal information. As per the PDPA, personal data encompasses any data that is connected to an individual either directly or indirectly which includes sensitive personal information such as data concerning the state of an individual's physical or mental health, along with their medical background and treatment-related details. Organizations that collect, process, or utilize health data are obligated to adhere to the fundamental principles of data protection as stipulated in the Act. This involves acquiring the individual's permission for the collection, processing, or utilization of their health data, and implementing suitable security precautions to safeguard the discretion and completeness of the data. This Regulation also includes provisions which confer special rights on individuals concerning their private details, e.g., the entitlement to retrieve and rectify data. related to health with respect to them as well as the prerogative to revoke consent for data processing. Organizations that violate the PDPA may be subject to fines and other enforcement actions by the Personal Data Protection Commissioner. In addition, individuals who have suffered harm because of a violation of the PDPA may be entitled to seek compensation through the courts. As per Section 5 of the Personal Data Protection Act (PDPA) of Malaysia, any individual or entity engaged in data processing in contravention of the core principles of data protection as defined in the Act is

committing an offense and is liable to a fine of MYR 300,000 or to imprisonment for 2 years or both. Organizations that collect, process, or use personal data must ensure that they comply with these principles, and failure to do so may result in a breach of the PDPA and the imposition of fines and other penalties. The duty of enforcing the PDPA and investigating complaints related to breaches or infringements of the Act lies with the Personal Data Protection Commissioner.

The main characteristics(similarities/differences) among the data privacy laws in above said countries and the draft bill of 2022 in India is as follows:

Table 4.2 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 that are obligated to comply with regulations, including 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

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.
Additional Health-Related Legislation	n/a	Health and Social Care Act 2012	n/a	n/a	n/a
Penalty	$25000-$1.5million.	€20 million	SGD 200,000	MYR 300,000	INR 500 Cr.

Qualitative Analysis of the interviews:

Thematic analysis was chosen for analysis as it is a commonly used method for analysis of qualitative data. A total of fifteen interviews were conducted with the policy makers. The following steps were followed for thematic analysis:

- Familiarization with the Personal Data Protection Bill:

  The Personal Data Protection Bill is a prospective legislation in India designed to govern the handling, retention, and transmission of individual information. The bill aims at enhancing the security of individuals' personal data and giving them more power to deal with their personal data. The provisions relate to collecting, using, and protecting individual data, the rights of individuals, their obligations as Data Controllers and how such legislation is enforced.

- Collection of Relevant Data:

  To analyze the Personal Data Protection Bill, data was collected from various sources such as government reports, and public opinions. Interviews were conducted with experts in the field of data protection to gain a better understanding of the key themes related to the bill.

- Identification of Themes:

  The interview transcripts from the policy makers and the bureaucrats were divided into the following themes regarding the characteristics of an effective digital personal data protection bill for India. The themes were selected based on the best practices done around the world for the protection of the healthcare data of the patients and how those practices can be implemented in India to make the digital personal data protection bill suitable to the requirements of the country.

  After analyzing the data, the following key themes related to the Personal Data Protection Bill were identified:

  - **Data Collection and Utilization:** This category encompasses concerns regarding the gathering and utilization of personal data by entities. It entails the requirement for organizations to acquire individuals' consent prior to gathering and utilizing their personal data, the permissible types of data collection, and the intended purposes for which such data can be utilized.

- **Privacy:** Personal data protection, as well as issues of privacy relating to individuals are addressed in this area. It covers several elements, including the right to have your personal data erased, access to information about you and notification in cases of privacy infringements.
- **Security:** The concept of security is accompanied by concerns about data protection. This implies the need for organizations to put in place appropriate security measures to ensure that no unauthorized access or disclosure of data is made.
- **Accountability:** The obligations of organizations responsible for processing personal data are subject to the concept of accountability. This means that organizations should comply with the obligation to provide transparency in their data processing operation, establish efficient complaints handling procedures and assume responsibility for any breaches or infringements of law.
- **Enforcement:** Enforcement includes issues pertaining to the enforcement of the Personal Data Protection Act. To ensure that organizations abide by the law and respect human rights, there is a need for robust enforcement mechanisms.
- **Cross-border data sharing:** Concerns about the transmission of personal health records within international borders are addressed in the Cross-boundary Data Transfer theme. It involves the obligation for organizations to abide by the data protection regulations of various jurisdictions and to implement appropriate measures to safeguard personal health data during such transfers.
- **Application of health data in research:** The theme of utilizing health data for research involves considerations regarding the utilization of an individual's personal health information for the purpose of conducting research. It involves the necessity for organizations to obtain clear and informed consent from individuals in an explicit manner prior to using their health data for research, and to put in place appropriate measures to assure the confidentiality and safety of personal health data are effectively maintained throughout the entire research process.

Conclusion:

From the analysis conducted, it can be inferred that the Personal Data Protection Bill remains an extensive legislation designed for safeguarding individuals' privacy and personal information. Nonetheless, certain aspects require further clarification, including the exact delineation of sensitive personal data and the obligations of social media companies. Additionally, it is advisable to establish efficient enforcement mechanisms to guarantee the effective implementation of the law.

Table 4.3 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.”
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.”

Chapter 5: 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.

- Initiative-taking 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 in lieu of the digital health ecosystem the Government of India is trying to create.

Chapter 6: Conclusion and Recommendations

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.

References:

1. Hackers attack Indian Healthcare website, Steal 68 lakh records: Report2 [Internet]. The Wire. 2019 [cited 2023 May 4]. Available from: https://thewire.in/health/hackers-attack-indian-healthcare-website-steal-68-lakh-records-report

2. Hackers attack Indian Healthcare website, Steal 68 lakh records: Report2 [Internet]. The Wire. 2019 [cited 2023Apr4]. Available from: https://thewire.in/health/hackers-attack-indian-healthcare-website-steal-68-lakh-records-report

3. Mittal A, Saxena H. Increased cyber-attacks on the global healthcare sector [Internet]. CloudSEK. 2022 [cited 2023 May 4]. Available from: https://uploadsssl.webflow.com/635e632477408d12d1811a64/63cfd7034745927b1c74ca2a_Increased-Cyber-Attacks-on-the-Global-Healthcare-Sector-WhitePaper-CloudSEK%20(1).pdf

4. Griffiths C. The latest Cyber Crime Statistics (updated March 2023): Aag it supports [Internet]. AAG IT Services. 2023 [cited 2023 May 4]. Available from: https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Cyber%20crime%20in%20India&text=In%20the%20first%202%20months,2020%20and%201%2C402%2C809%20in%202021.

5. Sanzgiri BV. 12.67 lakh cyber-attacks reported in India by November 2022: IT ministry in Parliament [Internet]. MediaNama. 2022 [cited 2023 Apr 4]. Available from: https://www.medianama.com/2022/12/223-12-67-lakh-cyber-attacks-reported-november-2022-meity/

6. HealthTech startups in India [Internet]. Tracxn. 2023 [cited 2023 May 7]. Available from: https://tracxn.com/explore/HealthTech-Startups-in-India

7. Ministry of Health and Family Welfare. Ayushman Bharat Digital Mission Draft Health Data Management Policy [Internet]. New Delhi (India). National Health

Authority;2022[updated April 2022; cited 2023 May 8]. Available from:https://abdm.gov.in:8081/uploads/Draft_HDM_Policy_April2022_e38c82eee5.pdf

8. Terry N. Existential challenges for healthcare data protection in the United States (2017)

9. Kharisma D, Diakanza A. Patient personal data protection: comparing the health-care regulations in Indonesia, Singapore, and the European Union (2022)

10. Costa A, Yelshyna A, Moreira T, Andrade F, Julian V, Novais P. A legal framework for an elderly healthcare platform: A privacy and data protection overview (2017)

11. MeiTY. Digital Personal Data Protection Bill [Internet]. New Delhi (India). Ministry of Electronics and Information Technology;2022[updated November 2022; cited 2023 May 8]. Available from:https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf

12. Information Commissioner Office. Data Protection and Digital Information Bill [Internet]. London (UK). Information Commissioner Office;2022[updated August 2022; cited 2023 May 9]. Available from: https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf

13. Text - H.R.8152 - 117th Congress (2021-2022): American data privacy and ... [Internet]. [cited 2023May8]. Available from: https://www.congress.gov/bill/117th-congress/house-bill/8152/text

14. Advisory guidelines on key concepts in personal data ... - PDPC [Internet]. [cited 2023May8]. Available from: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Oct-2021.pdf?la=en

15. Jabatan Perlindungan data peribadi [Internet]. Jabatan Perlindungan Data Peribadi. [cited 2023May4]. Available from: https://www.pdp.gov.my/jpdpv2/frequently-asked-questions/?lang=en

16. Georgiou D. Compatibility of a Security Policy for a Cloud-Based Healthcare System with the EU General Data Protection Regulation (GDPR) (2020).

17. Lalova-Spinks T, De Sutter E, Valcke P, Kindt E, Lejeune S, Negrouk A, et al. Challenges related to data protection in clinical research before and during the COVID-19 pandemic: An exploratory study. Front Med (Lausanne) [Internet]. 2022; 9:995689. Available from: http://dx.doi.org/10.3389/fmed.2022.995689

18. Galvin J, Suominen E, Morgan C, O'Connell E-J, Smith AP. Mental health nursing students' experiences of stress during training: A thematic analysis of qualitative interviews. Journal of Psychiatric and Mental Health Nursing. 2015;22(10):773–83.

19. Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006;3(2):77–101.

20. International AN. Data of organisations, 16.8 crore individuals stolen, six arrested [Internet]. NDTV.com. NDTV; 2023 [cited 2023 May 9]. Available from: https://www.ndtv.com/hyderabad-news/data-of-government-organisations-16-8-crore-individuals-stolen-6-held-3887088

21. Krishnakumar S. Cyber Crimes in India rise 6% a year in 2021, Telangana TOPS list: NCRB Data [Internet]. Moneycontrol. 2022 [cited 2023 May 9]. Available from: https://www.moneycontrol.com/news/india/cyber-crimes-in-india-rise-6-a-year-in-2021-telangana-tops-list-ncrb-data-9115161.html

22. Basuroy T. India: Number of cyber-crimes 2021 [Internet]. Statista. 2022 [cited 2023 May 9]. Available from: https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

23. National Crime Records Bureau. [cited 2023May8]. Available from: https://ncrb.gov.in/en/crime-in-india-table-addtional-table-and-chapter-contents?page=27

24. Anand A. Cyber-crime on rise, people's mindset and case registration are the problems: Explained [Internet]. cnbctv18.com. 2022 [cited 2023May8]. Available from: https://www.cnbctv18.com/india/cyber-crime-are-on-a-rise-in-india-amit-shah-cyber-security-ncrb-data-13913912.htm

25. Datta P, Panda SN, Tanwar S, Kaushal RK. A technical review report on cyber-crimes in India [Internet]. IEEE; 2020 [cited 2023May9]. Available from: https://ieeexplore.ieee.org/document/9167567/

26. Kumar PNV. Growing cyber-crimes in India: A survey | IEEE conference publication ... [Internet]. IEEE; 2016 [cited 2023May9]. Available from: https://ieeexplore.ieee.org/document/7684146

27. Muthuppalaniappan M, Stevenson K. Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to Global Health. International Journal for Quality in Health Care. 2020;33(1).

28. HIPAA Journal. 2022 Healthcare Data Breach Report [Internet]. HIPAA Journal. 2023 [cited 2023May4]. Available from: https://www.hipaajournal.com/2022-healthcare-data-breach-report/ .

29. Maqsood A, Rizwan M, Ahmad F. 1 average cost of data breach by country. - ResearchGate [Internet]. ResearchGate; 2019 [cited 2023May9]. Available from: https://www.researchgate.net/figure/Average-cost-of-data-breach-by-country_fig1_331715243 .

30. Ang A. 1.9 million cyberattacks against Indian Healthcare recorded in 2022 [Internet]. Healthcare IT News. 2022 [cited 2023 May 9]. Available from: https://www.healthcareitnews.com/news/asia/19-million-cyberattacks-against-indian-healthcare-recorded-2022#:~:text=ASIA-,1.9%20million%20cyberattacks%20against%20Indian%20healthcare%20recorded%20in%202022,an%20easy%20target%20for%20cybercriminals .

31. Rosenbloom ST, Smith JR, Bowen R, Burns J, Riplinger L, Payne TH. UPDATING HIPAA for the Electronic Medical Record Era. Journal of the American Medical Informatics Association. 2019;26(10):1115–9. doi:10.1093/jamia/ocz090.

32. Chua HN, Herbland A, Wong SF, Chang Y. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. Telematics and Informatics. 2017;34(4):157–70. doi: 10.1016/j.tele.2017.01.008.

33. Sudarwanto AS, Kharisma DB. Comparative study of personal data protection regulations in Indonesia, Hong Kong, and Malaysia. Journal of Financial Crime. 2021;29(4):1443–57. doi:10.1108/jfc-09-2021-0193.

Annexure:

Interview Questionnaire – Policy Makers, Subject Matter Experts and Bureaucrats

Name	
Age	
Designation	
Experience	
What are the characteristics of a good data protection bill in your opinion	
Should health data be segregated from other data	

Role of consent in data protection bill	
What happens to medical records and health data if a health facility is closed.	
Methods of protection from cyber-attacks & hackers	
Should heavy penalties be imposed on data breaches.	
Provision in bill if the hackers of data are based in another country	
How do you insure privacy in case of the bill	
What is new in the bill which is different from the bills of other countries	
Provisions for use of health data for research purposes.	