The Personal Data Protection Bill 2019 and Its Impact on The Healthcare Sector

Currently India does not have of an exhaustive data protection regime. Presently the **Sensitive Personal Data Rules, 2011** under the **Information Technology Act, 2000** hold the field**.** However, the rules have limited applicability as it imposes the obligations only on the body corporates.

With this background, The PDP Bill, introduced in **December 2019** is the government's second attempt at enacting a comprehensive data privacy regulation. The Bill -

- Seeks to regulate processing of personal data by Indian Government, companies incorporated in India, and by foreign companies dealing with Indian data principals.
- Provides for a separate regulation – Data Protection Authority of India.

Currently with the **Joint Parliamentary Committee** which is likely to submit its report in the second week of Winter Session.

Key Definitions under the PDP Bill

Under the bill, the following terms have been defined as follows:

- **Data Principal**: Natural person to whom the personal data relates.
- **Data Fiduciary**: Entity, including State, which determines the means and purpose of processing the personal data.
- **Data Processor**: Entity, including State, which undertakes the processing of personal data on behalf of the data fiduciary.

Classification of Data

Under the bill, data has been classified into Personal Data, Sensitive Personal Data and Critical Personal Data. Personal data refers to data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute, or any other feature of the identity of such natural person, and shall include any inference drawn from any such data for the purpose of profiling. Consent of data principal is required before processing.

Sensitive Personal Data means any such data which may reveal, be related to, or constitute: financial data, health data, sex life, sexual orientation, biometric data, official identifier, genetic data, religious and political belief, caste or tribe, any other data categorised as sensitive by government under s.15. Explicit consent of data principal is required.

Critical Personal Data means such personal data as may be notified by the Central Government to be the 25 critical personal data. This data can only be processed in India . Hence, cross-border flow of data is not allowed for the purpose of processing.

Regulation of Health Data

There have been several efforts to regulate health data. There has also been an attempt by Health Ministry to regulate health data under the draft **Digital Information Security in Healthcare Act (DISHA).** The Bill was never tabled and continues to remain in the draft stage. There is a mandate under the Clinical Establishments Act to maintain electronic health records.

Under PDP Bill, Health Data falls under the ambit of Sensitive Personal Data.

National Digital Health Mission (NDHM) and Data Protection Concerns

NDHM envisages a unique **Health ID Card** for every citizen. The card will contain confidential medical information including prescription, diagnostic reports, and discharge summaries – all stored in a digital format. NDHM would use the proposed National Health Stack – the digital health management framework to be used by both Centre and States across the public and private healthcare system. In August 2020, government released the health data management policy under NDHM. However, privacy experts maintain that a comprehensive data privacy regulation should be a pre-cursor to National Health Stack and NDHM. **In the absence of an enacted law and lack of data storage standards, there are concerns and fears of data breach, ineffective enforcement of rights of data principals, issues around data integrity, and collection of data without the consent of the patients.**

Indicative Compliance Challenges before Healthcare Organisations

Healthcare organisations deal with data with heightened sensitivity as compared to other industries. Data here includes patient healthcare records, biometric information, financial records, and health insurance information.

Compliance challenges for healthcare organisations include:

- Heightened compliance in the event healthcare organisation is categorised as a Significant Data Fiduciary.
- Implementing mechanisms for required data sharing with third parties in the supply chain.
- Implementing mechanisms for increased data transfer and sharing – under the envisaged digital health framework, it will be an interactive ecosystem.
- Increased compliance on General Practitioners to adhere to formats and standards while porting data.
- Liability of e-pharmacy websites at par with healthcare organisations.

Indicative Demands by the Healthcare Industry

In light of the above challenges, the Healthcare industry wants a separate privacy law. The industry wants graded compliance requirements based on the volume of data handled. This would mean that there would be increased compliance for chain of hospitals as compared to General Practitioners. The industry wants clarity on provisions for management of data following the death of the data principal and, on consent management during medical emergency. Considering the nature of practice, the

industry also wants a reduction in consent obligations for healthcare organisations. The industry wants a dedicated healthcare desk at the proposed Data Protection Authority. The industry is also seeking civil liability for offences instead of the criminal liability.

****

For further information, please reach out to us at info@borbhag.com

DISCLAIMER

- The information contained in this document has been compiled as of **September 2020** based on our secondary research and observations. The BORBHAG Group, its (direct or indirect) affiliates, directors, employees, agents, representatives or assigns, do not make any representation or warranty (express or implied) with respect to the information contained herein (including, without limitation, information obtained from third parties) and each of them expressly disclaim any and all liability based on or relating to the information contained in, or errors or omissions in / arising from, these materials; or based on or relating to the recipient's use (or the use by any of its affiliates or representatives) of these materials. The information contained herein is for general information purposes.
- The BORBHAG Group does not accept or assume any liability arising out of or in connection with use of this information.
- This information is not intended for distribution to, or use by, any person or entity in any jurisdiction or country where such distribution or use would be contrary to law or regulation.
- This information may contain confidential and / or proprietary information and may not be copied, loaned, or distributed to any other person. Please also note that the information contained herein has not been approved by any competent or regulatory authority and the same is subject to correction, completion, verification, and amendment. Recipients should not construe the contents of this document as legal or other advice.