Personal Data Protection Bill, 2019: Considering impact on the healthcare sector

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the tenth article in the series. Read our extensive coverage of the Bill here.

By Abhishek Malhotra and Bagmisikha Puhan

In the ambivalent situation that the healthcare sector finds itself in the middle of, the proposed data privacy and protection legislation lends direction to the stakeholders of this sector, that include healthcare providers, patients, caregivers, and other interested parties. The proposed legislation is timely, in that, the overlapping, co-dependent sectors, currently plagued with lack of uniformity in technical and organisational standards, will get the requisite impetus to align their approach and achieve efficiency in delivery of the services.

Section 2 (21) defines health data as *data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services.* In this present form, the proposed legislation encompasses the entire life cycle of a person's health information. The present healthcare set-up has evolved into a stage where the patients now prefer continuity of care, and their expectations regarding the preservation of health data/records ranges from womb to tomb.

Lack of data processing standards across the sector

In India, the healthcare set-ups are acutely heterogenous and do not interact with one another, which takes away from the end users the control over their own data, and the flow/management of their records. This extends beyond the care delivery set-ups, and also extends to the networks on which the product delivery platforms operate on (both brick and mortar, and online models).

While the proposed legislation deals with the creation, handling and management of personal and sensitive personal data, the Bill does not designate the individual (in this case, the patient) as the owner of the data pertaining to them. While the Bill's definition of data accounts for *representation, of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means,* the manner in which a General Practitioner (GP) in the country maintains records of his/her interactions with the patients are not in-line with the systems of a private hospital. Further, the proposed legislation assumes that the systems

within the ecosystem are capable of interacting with one another. That is not the way the healthcare sector operates in the country as healthcare providers, GPs and online platforms all use different technical standards. To facilitate seamless interactions across the sector, specific technical standards will have to be adopted/introduced.

Would a general practitioner and a hospital be equally liable?

The distinction between the compliance requirements of a GP and a larger hospital set-up would be in terms of the volumes of personal/sensitive personal data that is created and processed by the concerned entity. The concept of significant data fiduciaries (SDFs) would be attracted as per the levels of processing and would put the SDF in a position which requires stricter levels of compliance. Requirements like ensuring audits are conducted, and audit trails are maintained; along with the onerous, yet necessary, requirement of conducing a data protection impact assessment will be imposed on such hospitals. While this distinction will impact the level of compliance required of both the entities, the GPs will not be absolved of the requirements pertaining to confidentiality, integrity and accessibility of the personal/sensitive personal data sets. The GPs will have to ensure that they do not run afoul of the rights of the data principals, such as the right to access and to port the data to another healthcare service provider. When data is ported from an individual practitioner to a larger, organised set-up, homogeneity standards may come into play. The GPs would also need to comply with the requirements of provisioning of available data in a format/manner which is conducive for transfer from one unit to another in the best interests and at the instance of the data principal.

> **Is transferring patient records the same as porting data under right to portability?**
> Transfer of electronic health records, and electronic medical records qualifies as an extension of the right to portability whereby the data which may be sought to be ported must be raw data. For instance, assessment of health data will be inferred or derived data and may not fall within the scope of data portability, as with GDPR. Subject to further guidance, it will have to be evaluated whether data not provided by the data principal will be within the scope of this new right, and the extent as such.

The GP is expected to comply with the requirements prescribed under the proposed legislation, and must ensure that s/he relays and explains to new and existing patients the initiation of an interaction, continuation of treatment, and the expected consequences of such relationship created between the two individuals. Deriving from the expected National Digital Health Blueprint, the system is moving towards a synchronous and interactive framework, where the flow of information between the stakeholders is not restricted and is expected to be secure at all times. The National Digital Health Blueprint will have to

comply with the Bill once it becomes a law.

What happens in an emergency situation?

Going by how the sector operates in its current form, should a patient require urgent attention, it is upon the patient or his/her caregiver to bring in the old records to the hospital/clinic (formal set-up) for follow-up, validation, and further treatment. The Bill does not take away the requirements prescribed under the existing laws governing the healthcare sector. The Indian Medical Council (Professional Conduct, Etiquette, Ethics) Regulations, 2002, prescribes for the healthcare providers to maintain medical records in a desirable manner, and also urges for the computerisation of such medical records for quick retrieval. The proposed legislation is working in consonance with the existing approach and expects of all the stakeholders a similar level of compliance.

What happens when you order medicines or book diagnostics online?

For a user, the choice of consulting a physician from the options provided on the internet is based on the cost of the consult, availability of the physician and the location of the healthcare provider/ institution. All of these parameters are also accessible freely.

Most of these websites step beyond their designated roles of being facilitators and conduits to the more challenging role of an intermediary whereby they allow a user to book diagnostic tests, and to order medicines online. In doing so, the website needs to evaluate the prescription, which may be uploaded by the user directly, or may have been generated by the physician or consult made available by the website itself. In either scenario, the website is privy to the contents of such laboratory test results, diagnostic reports, prescriptions, and other captured information.

All of this information qualifies as sensitive personal data owing to the nature of the identifiers. **The liabilities of such a website will be similar to that of a data fiduciary which creates, consumes and processes personal/sensitive personal data in large volumes, and in all likelihood will qualify as an SDF.** The websites will be required to adhere to a certain level of technical and organisational standard which will be slightly higher than the standards prescribed for a GP. This will be owing to the number of processes and people who will be involved in processing the data pertaining to the large numbers of the end users. Further, the proposed legislation may lend further guidance in terms of the technical standards that the larger institutions will be subjected to, in contrast to what may be prescribed for a GP. **It is essential to note the difference that would exist between the ones employed by the GP and the ones deployed by the website, or a larger institution.** It is these nuances which will also impact the extent and the scope of liabilities that the entities will be subjected to, respectively.

Conclusion

Seemingly, there will be no additional riders under the proposed legislation, however, we may expect a guidance document or a policy document concerning the sector to come up for further understanding and effective implementation of the processes. However, in the meanwhile, the basic compliance requirements of proper and valid notices, explicit and specific consent, will have to be maintained and cannot be compromised by an individual practitioner, or a website.

The proposed legislation does not differentiate between the pedigree and the magnanimity of the data fiduciary on the basic compliance requirements. However, further compliance requirements are proposed in a manner which is proportional to the nature and scale of processing of personal and sensitive personal data of the individuals. **The liability that any entity will be subjected to under the proposed law will depend on the extent of the data being processed, the extent of dereliction and the effective controls which *supposedly* were in place for efficiency.**

*

Abhishek Malhotra *is the Managing Partner of TMT Law Practice. He has over 20 years of experience in dispute resolution and corporate advisory and actively participates in the development of policy and jurisprudence in the TMT sector, focusing on emerging technologies and the healthcare sector.*

Bagmisikha Puhan *is a Senior Associate at TMT Law Practice who specialises in technology law and advises clients in the ITeS, media, healthcare and pharmaceuticals, space sectors. A member of the Telemedicine Society of India, she also conducts capacity-building and training programmes. She has worked extensively in matters pertaining to the data privacy and data protection laws of several jurisdictions.*

Edited by Aditi Agrawal

*****Update (11:37 am): The headline was updated.*