Protecting Health Data under Digital Information Security in Healthcare Act (DISHA): A Case for COVID 19

W INVESTMENT
Finance. Law. Technology.

JULY 2, 2020

W-INVESTMENT
Shivani Agarwal
Samaksh Khanna

Background

Legislations protection data in India

In India, currently there is a lack of legal jurisprudence governing the general data protection let alone the protection of digital health data. In the past, the Ministry of Health had made an effort to protect the integrity of the health and medicare data of the patient by introducing the Digital Information Security in Healthcare Act (**"DISHA"**). It was sent to the Ministry of Electronics and Information Technology (**"MeitY"**) for comments, however, MeitY reverted stating that it was in the process of introducing Data Protection Framework on Digital Information Privacy, Security & Confidentiality' Act (**"DIPSC Act"**), which will subsume DISHA in order to avoid any duplicity of effort and shall be applicable across all sectors. Therefore, it can be assumed that there will be no sector specific data protection law in place in India as of now. Currently, the Personal Data Protection Bill, 2019 (**"PDP Bill, 2019"**) is up for discussion, however, the PDP Bill is a general data protection law applicable across all sector. It is unclear whether DIPSC Act will be a separate legislation and will co-exist with the PDP Bill.

Moreover, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 (**"SPDI Rules"**), governing the data protection framework in India, is not adequate to address all data security related issues. Under the SPDI Rules, it is possible for a 'body corporate' to have users agree to their privacy policy which may or may not meet the standards set in the SPDI Rules, therefore making the circumvention of the SPDI Rules possible.

Significance of a law can be measured by the penalties and fine imposed under such legislation. For the purpose of SPDI Rules, section 43-A of the Information Technology Act, 2000 (**"IT Act"**), specifies that the damages (in case of breach of consent or privacy) have to be paid as compensation. Between the PDP Bill and DISHA, penalty under PDP Bill is higher.

> ***"Under DISHA, the highest penalty is for a serious breach of digital health data or for data theft at INR 5 lakhs, while under PDP Bill, the maximum penalty imposed is INR 5 crores or 4% of the annual worldwide turnover, whichever is higher, for offences including breach of data localisation etc."***

Overview on DISHA

DISHA aimed to create a secure environment for the digital health care data and streamline the processing of such data. It proposed establishment of National Electronic Health Authority (**"NeHA"**) and State Electronic Health Authority (**"SeHA"),** who were to be the guardians of DISHA and formulate rules for data security and processing of heath care data. Further, DISHA proposed formulation of centrally established Health Information Exchanges (**"HIE"**), which would be responsible for collecting, storing and transmitting health data for the purposes specified in section 29 of DISHA which includes promoting research, detecting chronic diseases, guide medical decisions, etc. The data cannot be processed for the purpose for which either the consent of the owner is not given or there is no legal requirement. HIEs were to be directly regulated by NeHA and would be established by the central government. Section 31 of DISHA requires secure transmission of data from the clinical establishments to the HIE.

It is clear from the legislation that there will be multiple HIEs. However, DISHA, in the opinion of the authors, fails to consider the data breaches and leaks from such HIEs and even NeHA and SeHA. Breach of data from the national database is not unprecedented. The function of an HIE is merely that of an intermediary. Therefore, mandating the transmission of data to HIE may not be looked at positively. The procedure of exchange of data among the HIE was not specified in DISHA however could have been expected to be released via rules.

The main reason for introducing HIE into the system is to ensure interoperability of data. At numerous occasions, the patients are required to provide their data repeatedly upon every visit. The process for accessibility of data inter department, inter hospital, inter institutions and to the government is not streamlined. Several standard tests are conducted on a patient every time she visits the clinical establishment. However, this can be avoided through interoperability of the data which can reduce cost and fast tract the process.

DISHA establishes the HIE to ensure smooth transmission of data among all the stakeholders, including insurance companies. However, people may not trust such intermediaries with their data as sensitive as health data at all times.

Moreover, DISHA specifically disapproves the use of digital data for the purpose of commercialisation and cannot even be accessed by the insurance companies to process the claim unless the consent of the owner is obtained. Therefore, even if the health data is anonymised or de-identified, it cannot be used by such entities for the purpose of commercialisation.

DISHA and COVID 19

The data of the COVID 19 patients could squarely fall within the purpose stated in 29(1)(d), which reads as under:

"To improve public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks".

As per the proviso to the provision, the data for such a purpose can only be utilised, after it has been anonymised or de-identified, subject to the consent of the data owner. However, there might be instances when the data owner may not be in a position to grant any consent for collection of data in the first place due to her medical condition or mental condition, a 'proxy' consent shall be obtained from a nominated representative who has the capacity to consent. When the data owner regains consciousness or is able to grant consent, she shall have the right to withdraw the proxy consent and give her own consent. If the data owner agrees for the health data to be shared with any other entity, such entity shall be liable equal to the data collector for ensuring security and confidentiality.

Had DISHA been a legislation, the data collected by Aarogya Setu (**"App"**), a contact tracing application introduced by the government of India, would also have to comply, to the extent of generation, collection and retention of health data. Currently the privacy policy of the App does not have a sunset clause since the data can be retained by the government even after the purpose of tracing COVID19 and identifying cluster areas is served. A sunset clause ensures that the data will be deleted after a specific purpose is served. However, as per DISHA, the digital health data could only have been utilised for some specific purposes as listed down and could not have been kept open to its usage after the purpose is served unless the consent is obtained. DISHA does state that the data may be accessed or disclosed as required by the law or a statute, however, also provides a remedy if the data process was not in compliance. However, since no such law is in effect, data owners do not have a remedy in place against the government, in the event of misuse of their data.

Interoperability using blockchain

One of the main aims of establishing HIE was to ensure interoperability of data. Even though a sector specific legislation cannot be expected to be in place, advanced infrastructure for sharing data can be built once a general data protection law is in place. In order to build trust and secure space for transmission of health data to ensure interoperability, blockchain is the most optimum technology solution. The records stored on a blockchain are immutable and cannot be tampered with. The time stamp attached to the data ensure accuracy and transparency. A consortium blockchain can be adopted so the access can be given as and when required to the relevant stakeholders, upon receipt of proper and explicit consent. A record of such consent can also be stored on blockchain, using the smart contract mechanism, ensuring adequate data protection measures. Interoperability can only succeed if proper data protection norms are in place. People are less likely to trust interoperability if in the process, the sensitive or even critical nature of health data is commercialised for target advertisements or are processed for any purpose other than for which it was collected.

Author's Comments

During the pandemic of COVID-19, in many instances, lists of patients has been shared through messaging app WhatsApp, revealing the names, age and location of such patients. This is unethical and should also be deemed unlawful. A legislation like DISHA would have given the data protection of health care data a suitable direction. A general data protection law like the PDP Bill will possibly to be well complied with considering the penalties levied under it. However, it is the recommendation of the authors that the Data Protection Authority of India, to be established under the PDP Bill be encouraged to formulate rules for sensitive data related to health etc.

While it is not the case of the authors that there must be sector specific data protection laws, it is argued that the PDP Bill, 2019 must address the issues thoroughly and interests of stakeholders among all sectors should be kept at the center. Sector specific data authorities may be created but only for the purpose of supervising and not processing the data of the patients.