Page 3133 - 3141 **DOI:** *https://doij.org/10.10000/IJLMH.116485*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

Are Indians Medically Safe?: Inspecting the Problem of Data Security of Digital Healthcare Data in India

RUSHIKA BAKSHI[1]

ABSTRACT

The author in this paper has attempted to understand the hurdles faced by the Indian Healthcare sector due to its digitization. Medical information of a patient comes under the set of sensitive personal data and this research is aimed to understand whether the current Indian laws in force are strong enough to deal with data confidentiality and data privacy of such medical information. The paper further critically analyses the problem of data privacy in the Indian healthcare sector by understanding the various provisions contained in a number of statutes. The paper also brings into light an ideal legislation that should be enacted to minimize this issue and look after the rights of patients in respect of their sensitive medical data. Finally, the research proposes certain practices and measures to be followed by healthcare organizations in India in the absence of a proper legal framework so that they can keep a check on this problem and take steps to curb it.

Keywords: *Data Protection, privacy, security, sensitive medical data, Digital healthcare.*

I. INTRODUCTION

The world has become a digital economy and in this digital era all sectors are moving towards a paperless system wherein all information is collected and stored digitally. This rapid growth and development of technology has brought about not only the digitization of medical data of patients but also numerous e-medical technologies like health apps, online government health schemes and digital platforms providing health services. Due to the surge of electronic healthcare, digital storage of medical personal and sensitive data of patients has become exposed to potential risks. In India, the laws are quite incompetent to tackle the issue of data privacy in context of digital medical data particularly. The newly passed Digital Personal Data Protection Act, 2023 has completely done away with the idea of sensitive personal data and contains provisions only for personal data, thereby making digital medical data further unsafe. There is a legislation in the United States named as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which is a very complete law for protection of digital

[1] Author is a LL.M. Student at Jindal Global Law School, Sonipat, India.

 [ISSN 2581-5369]

medical data and a very similar legislation was proposed in India called as Digital Information Security in Healthcare Act (DISHA) but for the reasons best known to the government, the bill is not passed till date despite it being a quite effective statute. Due to the absence of any substantial statute for data protection of digital healthcare data in India, there are major threats lingering upon the security of such data of patients. So, all we can hope for is that health organizations in India comply with transparent and fair practices for collection, storage and use of such data[2].

II. UNDERSTANDING 'DIGITAL HEALTH' IN THE INDIAN CONTEXT

Simply put 'Digital Health' means using digital innovations and technologies for healthcare and it has become a significant subset of practicing medicine wherein new methods of information and communication are employed to address health related concerns[3]. Digital Health includes in its domain eHealth and mHealth. eHealth involves making use of latest information and communications technology for health. The most essential feature of eHealth is the Electronic Health Records (EHRs) which means consolidation of patient health information across all health organizations[4]. This was the first step for switching towards a paperless healthcare record and computerizing them. mHealth is public healthcare supported by mobile phones, electronic devices, digital patient assistants and wearables. Therefore, Digital Healthcare majorly comprises of two elements: digitization of personal and sensitive medical data and employment of technology for healthcare services.

After the breakout of COVID 19 pandemic, this concept has significantly taken shape in the India whereby the government collected medical and vaccine information of all citizens through Aarogya Setu and CoWin Applications. The government was regulating and processing medical data of people all across the country and further issued Telemedicine Practice Guidelines for medical practitioners during the pandemic. As per the published guidelines, doctors could consult their patients remotely through any medium including WhatsApp and internet-based platforms. Doctors had to strictly maintain patient teleconsultation records including e-prescriptions, reports and case history and they were prohibited from transferring or disclosing this data without the consent of the patient and were obliged to protect the privacy of the patient. But the excessive volume of data collected posed a serious concern and additionally the

[2] Nimisha Srinivas and Arpita Biswas, 'PROTECTING PATIENT INFORMATION IN INDIA: DATA PRIVACY LAW AND ITS CHALLENGES' [2012] NUJS Law Review 411.

[3] 'Introduction', *WHO guideline Recommendations on Digital Interventions for Health System Strengthening* (World Health Organization 2019) <https://www.ncbi.nlm.nih.gov/books/NBK541905/> accessed 5 November 2023.

[4] Janet Chan, 'Exploring Digital Health Care: eHealth, mHealth, and Librarian Opportunities' 109 Journal of the Medical Library Association: JMLA 376.

 [ISSN 2581-5369]

provision for obtaining express consent from the patient before transferring or disclosing his medical data lacked proper implementation. Further, ethical concerns were raised against the obtaining of express consent during teleconsultation from minors, people with mental or physical disabilities and people belonging to marginalized communities[5].

(A) Current Indian Legal Frameworks for Security of Digital Medical Data: A Quick Glance

In India, there is no one consolidated law for governing the data protection under the digital healthcare sector. Some health-related regulations make feeble efforts to target the aspect of data privacy and protection. Medical personal data is sensitive data and there should be additional safeguards for protection of this type of data but in the Indian framework, there is a major gap and absence of a robust law further triggers the issue.

The table below contains a list of laws, rules and regulations that throw little light on the protection of sensitive medical data of patients.

Legislation/Rules	**Provisions**
Information Technology Act, 2000	Section 2(1)(w) defines intermediary with respect to electronic records as any person who himself or on behalf of any other person stores, transfers or transmits that electronic record. Section 43A contains provisions for compensation when a body corporate fails in its responsibility to protect sensitive personal data stored in a computer. Section 79(3) states situations wherein intermediary will not be exempted from its liability.

[5] Dipika Jain, 'Regulation of Digital Healthcare in India: Ethical and Legal Challenges' (2023) 11 Healthcare 911.

 [ISSN 2581-5369]

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules)	Rule 3 states that sensitive personal data includes personal information like password, medical records and history, sexual orientation, physical or mental health condition, etc. Rule 4(1) mandates body corporates to issue a privacy policy with respect to handling sensitive personal data. Rule 5(1) directs the body corporate to derive consent from the provider relating to the purpose of usage of the data. As per Rule 5(3) the body corporate is duty bound to ensure that the individual is aware of certain things like: his information is being collected, recipients of such information, purpose for which it is so collected, etc. Rule 5(7) states that body corporates prior to collecting the sensitive personal data, shall provide the individual with the option of not giving this information. Rule 7 directs body corporates to ensure data protection while transferring sensitive personal data.
Digital Personal Data Protection Act, 2023 (DPDP Act)	Sections 4, 5 & 6 contain provisions regarding express consent of the Data Principal. However, the Act has completely done away with the notion of sensitive personal data unlike its previous drafts.
Clinical Establishments (Registration and Regulation) Act, 2010	Section 38(1) and 38(2) confer upon the state governments the duty to maintain digital electronic record of all clinical establishments of the state and forward it to the Central Government. And as per Section 39, Central Government shall maintain such digital record known as National Register of Clinical Establishments.

These legislations therefore are not sufficient and provide very little help in protection of digital medical data particularly. There is no standardized mechanism for obtaining express consent from the individual before collection, transferring or using his sensitive personal data. The only law in the country for protection of digital data that is the DPDP Act has completely disregarded the concept of sensitive personal data in its final draft and there is no distinction between

sensitive data and other data which additionally accelerates the problem as health data is not being considered as sensitive personal data.

(B) A Brief Look at some Government Initiatives for Digital Health Data

In 2020, the Central Government under its Ayushman Bharat Digital India Mission rolled out the National Digital Health Mission (NDHM) which was an initiative with a vision to curate a vast digital ecosystem which would enhance the effectiveness, transparency and efficiency of the Indian healthcare sector. As a part of the NHDM, every citizen was to be provided with a unique Health ID which is generated using individual data such as Aadhar number or mobile number and a biometric based identification number is created[6]. Thus, the NHDM aimed to generate a compiled digital repository of medical data of all Indian citizens in order to curb the problem of incomplete health records of patients and standardizing eHealth by including both personal data and sensitive personal data. However, NHDM suffers from certain major setbacks by way of opacity in the data collection process, no disclosure of the modes and mechanisms of data documentation and inadequately addressed procedures. Many Health IDs were autogenerated through the CoWIN platform using information of the account users without their knowledge or consent[7]. Such normalization in collecting sensitive personal data poses serious privacy concerns. The National Health Authority came up with Health Data Management Policy which had to be complied with by all the partakers of the Digital India Mission. The policy had rules like individual's right of access to information, right to erasure and limitations on collection, transmission, storage and usage of data but this policy lacks effectiveness and does not have any statutory legitimacy[8].

III. INDIA'S PROPOSED LAW ON DIGITAL SECURITY IN HEALTHCARE- 'DISHA'

In the United States, there is a legislation in practice called the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which is a set countrywide legal framework for privacy of healthcare information[9]. Under the said act the Department of Health and Human Services is set up which further issued privacy rules and security rules. The Act and the Rules in consolidation provide patients with a number of rights including protection of data from unauthorized access, no disclosure of data without authorization of the patient, requesting

[6] ibid.
[7] Smriti Parsheera, 'As Health Goes Digital in India, Where Does Privacy Stand?' (*Scroll.in*, 20 March 2023) <https://scroll.in/article/1045509/as-health-goes-digital-in-india-where-does-privacy-stand> accessed 6 November 2023.
[8] ibid.
[9] Linda Koontz, 'Health Information Privacy in a Changing Landscape' (2015) 39 Generations: Journal of the American Society on Aging 97.

 [ISSN 2581-5369]

correction of information, right to know where the data is being used, etc[10].

A similar robust legislation was proposed in 2018 but unfortunately it stands as being not passed till date. The consolidated Act proposed by the Ministry of Health and Family Welfare (MoHFW) is called as the Digital Information Security in Healthcare Act (DISHA). DISHA lays down a comprehensive framework for collection, transmission, transfer, access, storage and use of two types of data: Digital Health Data and Personally Identifiable Information[11]. According to the proposed act, 'Digital Health Data' includes electronic record of health-related information of an individual which comprises of information about mental and physical health, health services provided, donation of any body part and details collected in the course of providing healthcare services[12]. Whereas, Personally Identifiable Information includes any information which can be used to precisely identify, locate or contact any individual[13].

DISHA much like the HIPAA confers a wide range of rights upon the patients which include:

- Right to confidentiality, privacy and security of digital healthcare data which is collected, transmitted or stored.
- Right to give and withdraw consent for data collection.
- Right to deny the disclosure or access to his digital medical data.
- Right to be notified when data is being accessed.
- Right to seek compensation in case of data breach.
- Right to prevent transmission or disclosure of sensitive health data.
- Right to know the purpose for which the data is being collected, transferred or transmitted.
- Right to rectify and correct the digital health data.
- Right to ensure that in case of emergencies, data is being shared only with the family members or only with such persons specified by the patient.

DISHA also stipulates the particular purposes and uses of digital healthcare data and the data

[10] Robert Lord and Dillon Roseen, 'Why Should We Care?' (New America 2019) <http://www.jstor.org/stable/resrep19972.6> accessed 5 November 2023.
[11] 'DISHA – India's Probable Response To The Law On Protection Of Digital Health Data - Healthcare - India' <https://www.mondaq.com/india/healthcare/1059266/disha--indias-probable-response-to-the-law-on-protection-of-digital-health-data> accessed 6 November 2023.
[12] Section 3(e) of DISHA,
'R_4179_1521627488625_0.Pdf'
<https://main.mohfw.gov.in/sites/default/files/R_4179_1521627488625_0.pdf> accessed 5 November 2023.
[13] Section 3(k) and Schedule 1 of DISHA
ibid.

 [ISSN 2581-5369]

should be used only for medical purposes, to identify the threats of any underlying disease, for diagnosis, to improve public health and to carry out academic research, analysis and policy formulation[14]. The data should be disclosed only for treatment or healthcare related services and the information disclosed must be as minimum as necessary to perform a specific task. DISHA also mandates the health organization to undertake security measures to prevent misuse of data.

DISHA bifurcates data breach into two parts: Breach of Digital Health Data in which the wrongdoer will be liable for compensation and Serious Breach of Digital Health Data which punishes the offender with imprisonment that can extend from three to five and also with a minimum fine of five lakh rupees.

But most importantly, DISHA contain provisions for establishment of National Electronic Health Authority (NeHA) at the central level and State Electronic Health Authorities at the state level to control and supervise the day-to-day functions of all health organizations related to the transfer, collection and transmission of digital medical data[15]. These authorities have a duty to secure an individual's personal medical data and maintain confidentiality throughout the process of providing healthcare services. They are expected to function in a transparent manner and also conduct investigation in cases relating to breach and non-compliance[16].

DISHA therefore was a very focused step put forward by the MoHFW which ensures the protection of HER and confidential medical information, by furthering a robust mechanism and empowering the individuals with numerous rights just like the HIPAA of the United States. Implementation of DISHA and establishment of NeHA will build a concrete pathway for India to curb the hanging problem of lack of any substantial legislation for security and privacy of digital health data.

IV. MEASURES TO ADOPT WHILE DISHA IS STILL UNDERWAY

While there is no clarity as to when the DISHA Act might be passed by the legislature and be functional, in the meantime there are certain practices which might reduce the problem if not completely eliminate it.

- User Authentication on Web and Online Health Applications so that only authorized

[14] Compliancy Group, 'DISHA and HIPAA, How Do They Compare?' (*Compliancy Group*) <https://compliancy-group.com/disha-and-hipaa-how-do-they-compare/> accessed 6 November 2023.
[15] Law Essentials, 'Digital Information Security in Healthcare Act, 2018' (*Law Essentials*) <https://lawessential.com/m%26a-deals-%26-cases-archive/f/digital-information-security-in-healthcare-act-2018> accessed 5 November 2023.
[16] Puneetha Choudhary, 'Digital Information Security and Privacy Protection in Healthcare Sector in India' (2022) 4 Issue 2 Indian Journal of Law and Legal Research 1.

account holders are able to access the secured data and the access to such data is restricted for unauthorized users. There is a need for strengthened access control policy with can be incorporated by using features like encryption, strong passwords, two factor authentication, firewall and antivirus[17].

- A consent form for patients and individuals to obtain their consent for usage, collection and storage of their sensitive healthcare data and also providing them with the option of not providing such consent.
- Health organizations should function in a fair and transparent manner and their privacy policies should be made available to individuals.
- Personal medical records should be disclosed only to those persons who have a right to know and those who are authorized by the patient.
- Data minimisation: collecting only that much data as would be required.
- Notifying the individual in case of data breach.
- Coming up with a standardized format for recording patient's medical information[18].
- Implementing strong control mechanisms on data usage so as to look into the problem of data misuse and data breach.
- Educating the healthcare sector workers and staff and acquainting them with digital literacy, computer literacy and imparting knowledge about proper handling of patient's digital medical data.
- Establishing a proper grievance redressal mechanism and an independent agency that can look into grievances and complaints relating to sensitive personal data.

V. CONCLUSION

Protection of health data under current statutes is very generic in nature and there is a lack of any comprehensive law. However, SPDI Rules, 2011 do give an overview of security and disclosure of sensitive personal data but it is not a comprehensive robust legislation which only deals with data protection of digital healthcare data. Therefore, there is a need of a statute like DISHA in India which can help to overcome the problem digitization of healthcare sector. But this does not mean that healthcare organizations at present can do nothing to better the situation

[17] Natasha Vaz, 'Health Privacy in India: A Legal Mapping' (23 June 2014) <https://papers.ssrn.com/abstract=2457959> accessed 5 November 2023.

[18] Amrutha K., 'Digital Healthcare during COVID-19 Pandemic: Application and Regulatory Aspects of Telemedicine' (2021) 2 Indian Journal of Law and Legal Research 1.

 [ISSN 2581-5369]

at hand. There are certain suggested mechanisms which if implemented can reduce the gravity of the problem and address the data privacy concerns of individuals. The introduction of DISHA was a very positive step and there is hope that in the near future it shall be implemented. Further establishment of a body like NeHA as a regulatory authority would make India one of the prominent countries successfully regulating sensitive healthcare data.

*****

 [ISSN 2581-5369]