
INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DATA PROTECTION AND IMPACT ON MEDICAL PRACTITIONERS- Zorawar Singh Rathore¹**Abstract**

With an emphasis on the Digital Personal Data Protection (DPDP) Act, 2023, and its consequences for medical professionals, this article conducts a thorough analysis of the significant effects of India's quickly changing data protection environment. It emphasises how urgently a unified, standardised, and legally binding framework to control the gathering, handling, storing, and sharing of private patient data is needed. Inconsistencies, uncertainty, and frequent breaches of patient confidentiality among healthcare institutions are currently the outcome of the lack of a unified system. The article explores how the Act has changed the roles and obligations of medical professionals as data custodians, emphasising how important it is to get patients' express, informed, and unqualified consent before processing any personal health data. It also highlights the necessity of following legal and moral guidelines while managing data and putting strong organisational and technical measures in place to stop breaches. The report also outlines the legal requirements put on healthcare providers, particularly those pertaining to data breach notifications, and addresses the specific exceptions to the duty of patient confidentiality, such as disclosures required by the public interest or court orders. In order to show how seriously the legislation takes protecting patient privacy, the report also describes the severe consequences that medical professionals may encounter for non-compliance. The article comes to the conclusion that incorporating open, consent-driven, and legally compliant data management procedures is critical for preserving patient privacy, upholding the fundamental right to privacy guaranteed under the Indian Constitution, and preserving public confidence in the healthcare system.

Keywords: - Data Protection; DPDP Act 2023; Medical Practitioners; Privacy Rights; Patient Consent.

Introduction

¹ Student at Himachal Pradesh National Law University, Shimla.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

In India, the handling of patients' medical data by medical practitioners is fraught with significant privacy concerns, particularly during the transfer of data from one department to another, even when such transfers are for legitimate medical reasons. While many hospitals, doctors, private clinics, and other healthcare providers may have internal systems in place that aim to maintain the privacy of patient information during processing, these systems often lack uniformity and legal backing. The current approach relies heavily on the subjective "reasonable person" standard when resolving disputes concerning breaches of medical privacy, which leads to ambiguity and a lack of accountability. There is an urgent need for a standardized, legally enforceable framework that governs the collection, processing, and sharing of medical data across all levels of healthcare services. Such a framework must be backed by statutory regulations to ensure consistent implementation and provide recourse in case of violations. The recently enacted Digital Personal Data Protection (DPDP) Act, 2023 offers a valuable blueprint in this regard, as it outlines clear obligations for data fiduciaries and processors regarding the management of personal data. Medical practitioners could adopt similar legislative measures that not only define how patient data should be processed and transferred but also impose penalties on those who mishandle such sensitive information. A legally monitored and uniform system will help safeguard patients' right to privacy and restore trust in the healthcare ecosystem.

Medical Practitioner and Patient

Section 2 (j)² and section 2(i)³ of the Act includes or legislates or provides about the Data Principal whose data is being processed (i.e. the Patient), and the Data Fiduciary who is responsible for processing the personal data (i.e. Medical Practitioner). The Data Principal can be any type of patient which includes an adult, a minor, or a person with disability.

What kind of Data?

The term 'data' refers to any representation of information, facts, concepts, opinions, or instructions that can be communicated, interpreted, or processed by humans or automated systems⁴, this includes any kind of medical information that the patient shares with the medical practitioner like the history of the patient, the medical reports, allergies, or any other relevant details, etc.

² The Digital Personal and Digital Protection Act, 2023, §2(j).

³ The Digital Personal and Digital Protection Act, 2023, §2(i).

⁴ The Digital Personal and Digital Protection Act, 2023, §2(h).

Requirement of Explicit Consent

It is very explicitly clarified that the Data Principal or the Patient must give explicit consent for processing his or her personal data and such consent must be used for legitimate use.⁵ The term 'legitimate use' refers to ethical, and medically justified application of the patient information within a hospital setting, in accordance with prevailing standards provided by the relevant authorities. It is also stated that the consent given by the Patient to the Medical Professional shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. Additionally, where the Patient is a minor or a person with disability, such consent shall be given by the parent or the legal guardian of the patient to the medical practitioner.⁶

Processing of Personal Data and Notice

The personal data must be processed as per the provisions of the Act and for a lawful purpose only.⁷ It is well stated that every request made to a Patient under section 6 for consent shall be accompanied or preceded by a notice given by the Medical Practitioner to the Patient, informing her about the personal data and the purpose for which the same is proposed to be processed; the manner in which she may exercise her rights; and the manner in which the patient may make a complaint.⁸ Additionally, Section 7 specifies that data can be processed for "certain legitimate uses" on the condition that the patient has voluntarily provided her personal data to the medical practitioner, and "has not indicated to the Data Fiduciary that she does not consent to its use".⁹ It was also held in the case of *Mr 'X' v. Hospital 'Z'*¹⁰ that,

"12. It is true that in the doctor-patient relationship, the most important aspect is the doctor's duty of maintaining secrecy. A doctor cannot disclose to a person any information regarding his patient which he has gathered in the course of

⁵ The Digital Personal and Digital Protection Act, 2023, §6.

⁶ The Digital Personal and Digital Protection Act, 2023, §9.

⁷ The Digital Personal and Digital Protection Act, 2023, §4.

⁸ The Digital Personal and Digital Protection Act, 2023, §5.

⁹ The Digital Personal and Digital Protection Act, 2023, §7.

¹⁰ *Mr 'X' v. Hospital 'Z'*, (1998) 8 SCC 296 (India).

treatment nor can the doctor disclose to anyone else the mode of treatment or the advice given by him to the patient.

13. It is contended that the doctor's duty to maintain secrecy has a correlative right vested in the patient that whatever has come to the knowledge of the doctor would not be divulged and it is this right which is being enforced through these proceedings.", therefore showing the importance of maintaining secrecy of the personal data of the patient by the medical practitioner."

However in the very same case it was held that,

"14. It is the basic principle of jurisprudence that every right has a correlative duty and every duty has a correlative right. But the rule is not absolute. It is subject to certain exceptions in the sense that a person may have a right but there may not be a correlative duty. The instant case, as we shall presently see, falls within the exceptions.

16. The Hippocratic oath as such is not enforceable in a court of law as it has no statutory force. Medical information about a person is protected by the Code of Professional Conduct made by the Medical Council of India under Section 33(m) read with Section 20-A of the Act. The relevant provisions of the Code of Medical Ethics have already been reproduced above which contain an exception to the general rule of confidentiality, inasmuch as it provides that the information may be disclosed in a court of law under the orders of the Presiding Judge. This is also the law in England where it is provided that the exceptions to this rule permit disclosure with the consent, or in the best interests, of the patient, in compliance with a court order or other legally enforceable duty and, in very limited circumstances, where the public interest so requires. Circumstances in which the public interest would override the duty of confidentiality could, for example, be the investigation and prosecution of serious crime or where there is an immediate or future (but not a past and remote) health risk to others."

Hence, this shows that such right to privacy is not absolute with respect to public interest and the respective personal data can be processed accordingly. It was also held in the case of *Tokugha Yephthomi Vs. Apollo Hospital Enterprises Ltd.*¹¹ that,

"26. As one of the basic Human Rights, the right of privacy is not treated as absolute and is subject to such action as may be lawfully taken for the prevention

¹¹Tokugha Yephthomi v. Apollo Hospital Enterprises Ltd., MANU/SC/2214/1998 (India).

of crime or disorder or protection of health or morals or protection of rights and freedoms of others.

27. Right of Privacy may, apart from contract, also arise out of a particular specific relationship which may be commercial, matrimonial, or even political. As already discussed above, doctor-patient relationship, though basically commercial, is, professionally, a matter of confidence and, therefore, doctors are morally and ethically bound to maintain confidentiality. In such a situation, public disclosure of even true private facts may amount to an invasion of the Right of Privacy which may sometimes lead to the clash of one person's "right to be let alone" with another person's right to be informed.

28. Disclosure of even true private facts has the tendency to disturb a person's tranquility. It may generate many complexes in him and may even lead to psychological problems. He may, thereafter, have a disturbed life all through. In the face of these potentialities, and as already held by this Court in its various decisions referred to above, the Right of Privacy is an essential component of right to life envisaged by Article 21. The right, however, is not absolute and may be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others.”

Obligations of the Medical Practitioner towards the Patient

The obligation of the medical practitioner under section 8¹², recognises the liability and responsibility of the medical practitioner as per the provisions of the Act. It also states the following:-

- A medical practitioner may engage, appoint, use or otherwise involve a Data Processor to process personal data on its behalf for any activity related to offering of goods or services to patient only under a valid contract.
- A medical practitioner shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of the Act and the rules made thereunder.
- Also, a medical practitioner shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its

¹²The Digital Personal and Digital Protection Act, 2023, §8.

behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.

- It is obligatory for the medical practitioner to inform the patient in case of breach of personal data in a prescribed form or manner.
- It should also be noted that, a patient shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force,¹³ therefore, upon receiving a request for correction, completion, updating or erasure, the following request will be complied with by the medical practitioner.

Section 7 of the Act also specifies that the medical practitioner can process the data of the patient in cases where-

- Adhering to any ruling, decree, or order issued under any currently enacted Indian legislation, as well as any ruling or order pertaining to civil or contractual claims under any currently enacted foreign law.
- Addressing a medical emergency that poses an urgent risk to the Data Principal's or any other person's life or health.
- Taking action to offer medical care or health services to everyone in the event of a disease outbreak, epidemic, or other public health emergency.
- Taking action to guarantee someone's safety or to offer them support or services in the event of a calamity or a breakdown in public order.
- For the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.

Impact of non-compliance by the medical practitioner

The patient will always have the right to grievance redressal provided by the medical practitioner regarding the performance of its obligations in relation to the personal

¹³The Digital Personal and Digital Protection Act, 2023, §12.

data or the exercise of her rights under the provisions of the Act and the rules made thereunder.¹⁴ Additionally, the Schedule of the Act specifies the penalty of the medical practitioner.¹⁵ The schedule states that-

- A violation of the Data Fiduciary's duty to implement appropriate security measures to prevent the breach of personal data under sub-section (5) of section 8 may result in a fine of up to 250 crore rupees.
- A violation of the requirement to notify the Board or the impacted Data Principal of a breach involving personal data under sub-section (6) of section 8 may result in a fine of up to two hundred crore rupees.
- A violation of the additional duties pertaining to minors under section 9 may result in a fine of up to two hundred crore rupees.

Exemptions against general obligation to process personal data

There are some exemptions mentioned under section 17 of the Act¹⁶ that talk about the processing of personal data by the Data Fiduciary or the medical practitioner where the general obligations will not apply. They are as follows:-

- Processing personal data is required to enforce any legal claim or right.
- The processing of personal information by any Indian court, tribunal, or other entity authorised by law to carry out judicial, quasi-judicial, regulatory, or supervisory functions, if such processing is required to carry out such functions,
- The processing of personal information is done to prevent, detect, investigate, or prosecute any offence or violation of any current Indian legislation,
- Personal information of Data Principals who are not located in India is processed in accordance with any agreement that an Indian-based individual enters into with an individual outside of India,
- If a court, tribunal, or other authority authorised by any currently enacted law has approved a scheme of compromise, arrangement, merger, or amalgamation of two or more companies, a reconstruction of a company through demerger or otherwise, a transfer of undertaking of one or more companies to another

¹⁴The Digital Personal and Digital Protection Act, 2023, §13.

¹⁵The Digital Personal and Digital Protection Act, 2023, The Schedule.

¹⁶The Digital Personal and Digital Protection Act, 2023, §17.

company, or involving the division of one or more companies, the processing is required, and

- If the processing complies with the provisions pertaining to information or data disclosure in any other currently enacted law, it will be used to determine the financial information, assets, and liabilities of any individual who has fallen behind on payments owed on account of a loan or advance obtained from a financial institution.

Conclusion

A thorough, standardised, and legally enforced data protection framework that is specifically suited to the medical industry is urgently needed, as can be seen by examining the entire Act. Although the DPDP Act of 2023 offers a strong legal foundation for processing personal data, medical practice requires that its tenets be successfully modified and applied. As data fiduciaries, medical professionals have an ethical and legal obligation to make sure that patient data is gathered, processed, stored, and shared in a way that respects confidentiality and privacy. Inconsistencies and accountability breakdowns have long been tolerated due to the absence of a centralised system and the dependence on arbitrary criteria such as the "reasonable person" test. Incorporating the DPDP Act's provisions into healthcare procedures will protect patients' fundamental rights under Article 21 of the Constitution while also fostering greater confidence between patients and healthcare providers. Additionally, the Act serves as a deterrence against improper management of sensitive medical data by outlining severe consequences for violations and non-compliance. Therefore, it is essential that all parties involved in the medical ecosystem that is to say hospitals, clinics, private practitioners, and regulatory agencies must adopt transparent, consent-based, and legally compliant data protection procedures. Only then will we be able to guarantee that the right to privacy is effectively safeguarded, particularly in a field as sensitive and private as healthcare.