Confidentiality Issues in Indian Healthcare Data Management

By Sanjana Chandran Kowshik* & Dr Chaitra Rangappa Beerannavar**

** LLM Student, School of Law, Christ (Deemed to be University), Bangalore, Karnataka, India*

*** Associate Professor, School of Law, Christ (Deemed to be University), Bangalore, Karnataka, India*

Abstract

The article presents a thorough examination of the regulatory structure concerning confidentiality in the doctor-patient interaction in India. It emphasises the lack of particular laws addressing this matter, despite its crucial significance. This study examines the principles specified in the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Rules, 2002, with a focus on the ban of revealing patient information and the resulting repercussions for violations.

Furthermore, the article explores the planned Digital Information Security in Healthcare Act (DISHA), which seeks to create national and state eHealth agencies and health information exchanges. Although not yet implemented, DISHA aims to provide uniform standards and regulations for the gathering, retention, transfer, and use of digital health information, with a particular emphasis on safeguarding data privacy and security.

The article additionally examines the Puttaswamy judgement and its ramifications for data security and privacy in India, specifically in relation to the Aadhar programme. The article next analyses the Digital Personal Data Protection Act, 2023 (DPDP Act), which came into effect on January 1, 2024. The DPDP Act seeks to govern the handling of personal data, including health information, and imposes strict requirements on data fiduciaries. It may be compared to the EU's General Data Protection Regulation (GDPR). The text examines the influence of the DPDP Act on the management of healthcare data, highlighting the need for strong

cybersecurity measures, data governance frameworks, and compliance standards within the healthcare industry.

The article emphasises the changing situation of confidentiality in particular as well as data privacy with the help of regulatory framework in India's healthcare industry, focusing on the difficulties and possibilities brought about by new laws and technological progress.

Keywords – Confidentiality, Doctor-Patient relationship, healthcare data, privacy, DPDP Act.

Introduction

The doctor-patient relationship (DPR) is regarded as the key component in the medical field. DPR is often established and begins when a doctor provides medical care to a patient in a pleasant way, including but not limited to check-ups, diagnosis, and treatment. Due to the doctor-patient connection, the doctor has a responsibility to effectively cure the condition or terminate the partnership based on the ethics. At the very first stage itself, every doctor must establish a satisfying Doctor-Patient Relationship (DPR) to provide exceptional healthcare to patients.

The Doctor-Patient Relationship always carries along with it private and sensitive information (like medical history or the finances), and therefore the very concept of confidentiality in this relationship facilitates honest, frank, no filter and transparent communication between the doctor and patient. Medical confidentiality is the practice of doctors keeping all information received during the course of a patient's treatment private.[i] This sort of attitude fosters the growth of the much necessary fiduciary relationship between the doctor and concerned patients in order to avail the best medical services going forward. Consequently, anonymity plays a crucial role in every DPR in order to balance the interests.

However, placing trust and faith in a doctor’s ability to safeguard confidential information can be really challenging. Therefore, the principle of confidentiality plays a crucial role in fostering and preserving a patient’s trust in the medical process. It allows patients to feel secure in divulging personal details and experiences that they may otherwise feel hesitant to discuss. As rightly put by therapist Kamna Chhibber while defining confidentiality,[ii] “It is not just related

to the content of what may be discussed in a therapy session but also the fact that a client is in therapy with a therapist."

In common law[iii], concept of confidentiality didn't exist to protect any sort of information exchanged between the doctor and the patient.[iv] Back in those days, the need hadn't arisen as every family had a their own family doctors and they hardly made any disclosure of the individual's medical history.[v] But in today's contemporary world, it is not hidden that the shared sensitive data of patients has been time and again misused by the data fiduciaries which makes it necessary for the government to enact regulations governing the very concept of confidentiality of data especially in the field of medicine.

Through the safe storage of medical records and the prevention of their exposure to the general public, right to privacy protects the patient's right to privacy and the secrecy of their identity. The patient has the right to take legal redress in the event that sensitive medical information is provided to a third party that is not entitled to receive it, and the patient's identity is divulged without the patient's agreement.[vi]

On the other hand, specific to the realm of data is the concept of confidentiality. The phrase "medical confidentiality" refers to the right of an individual to have their personal and identifiable medical information kept private and shared solely between the patient and the practitioner. This privilege is referred to as "medical confidentiality." This idea is either a continuation of the notion of privacy or an augmentation of it.[vii]

Doctor-Patient Privilege of Confidentiality - Objectives

General public health and patient's privacy are the two major driving forces for the establishment of Doctor-Patient Privilege in the first place.[viii] The doctor-patient privilege, originally established to serve the public health purpose, is rooted in the concept that maintaining the confidentiality of medical information is crucial for promoting public health.[ix] This is because the fear of medical data being disclosed may deter patients from obtaining necessary medical care.[x] By guaranteeing patients that whatever information they provide with the doctor will be kept secret, they will feel more inclined to openly provide the required details

for an accurate diagnosis and effective treatment of their disease or injury. Failure to disclose certain vital information may impact the effectiveness of medical care, the trust between physician and patient, and the accuracy of the medical records.[xi]

The veracity of the public health reasoning is now under doubt.[xii] It is widely believed that most patients who get treatment from a doctor are mainly focused on the effective treatment of their sickness and are not worried about the remote possibility of their medical condition being disclosed in court at a later time.[xiii]

According to Professor Morgan:

"The ordinary citizen who contemplates consulting a physician not only has no thought of a lawsuit, but he is entirely ignorant of the rules of evidence. He has no idea whether a communication to a physician is or is not privileged. If he thinks at all about the matter, he will have no hesitation about permitting the disclosure of his ailments except in a case of a disease which he considers disgraceful,"[xiv]

Supporters of Professor Morgan argue that if the guarantee of confidentiality has little impact on a patient's willingness to seek medical care, then the public health justification alone is insufficient to warrant the legal protection of doctor-patient confidentiality.[xv]

Confidentiality encompasses two fundamental rights: the right of an individual to have authority over the release of personal information, and the right of an individual to make personal choices without interference from the government.[xvi] Although the public health justification is becoming less strong, the right to privacy remains a compelling argument for maintaining the doctor-patient privilege. The courts must not unjustly or arbitrarily violate an individual's private rights, since these rights are substantial.[xvii] Moreover, although many courts have acknowledged the constitutional right of patients to privacy with respect to their medical information, there is considerable uncertainty about the scope and interpretation of this right.[xviii]

However, some individuals see the privilege as a disadvantage rather than a benefit.[xix] According to retired California Judge B. Abbott Goldberg, the physician-patient privilege might potentially do significant damage. He argues that preserving this privilege allows

individuals to establish a basic and defendable right to privacy in order to protect themselves from fraudulent and incompetent healthcare providers.[xx] He said that there is no evidence to demonstrate that the exceptions to the privilege have caused any patient's significant damage. This fact supports the idea that the privilege is founded on a simple notion.7 Judge Goldberg believed that the protected position may be exploited, since it could operate as a barrier to shield dishonest practitioners from legal action.[xxi]

Psychotherapist-Patient Relationship Confidentiality

Similar to doctor-patient interactions, several issues occur when it comes to revealing sensitive information in the psychotherapist-patient relationship. Several jurisdictions have implemented laws safeguarding the interactions between patients and their psychiatrists, psychologists, and social workers.[xxii] The privilege grants the patient the freedom to engage in unrestricted communication with their psychotherapist. The inherent characteristics of psychotherapy intervention warrant a significant level of secrecy, which may be more essential for the management of a mental disorder than safeguarding medical data alone cannot assist him. Complete transparency about the patient's deepest feelings, anxieties, and imaginative thoughts is an essential need for successful therapy, and the patient must actively participate in the management of a bodily ailment.[xxiii] The patient had treatment from a doctor whom they did not trust, yet a psychologist must gain the trust of their patient in order to fairly assume that the patient's confidential information would be kept private.[xxiv]

The psychotherapist must establish themselves as the patient's most reliable and confidential advisor. While the physician-patient privilege may not always be justified, the psychotherapist-patient privilege is consistently supported and justified by the public health purpose.[xxv] Without the assurance of confidentiality, individuals may hesitate to promptly seek therapy or freely share their thoughts and feelings with a psychotherapist.[xxvi]

But the relation between doctor-patient and psychotherapist-patient vary by a blur line. The sensitive nature of the interactions in the psychotherapist-patient relationship necessitates the utmost secrecy, and a psychotherapist may face challenges in their professional role if they are unable to guarantee their patients confidentiality in their conversations.[xxvii] According to the

Group For the Advancement of Psychiatry, confidentiality is an essential need for effective therapy.[xxviii] The psychotherapist-patient privilege seeks to uphold the human dignity of individuals who willingly expose themselves to extreme vulnerability in their pursuit of enhanced mental well-being via the therapeutic process.[xxix] The privilege of psychotherapist-patient confidentiality, similar to the privilege of doctor-patient confidentiality, is not an unconditional entitlement and may be set aside in certain circumstances to facilitate the pursuit of truth in legal proceedings.[xxx] Courts weigh the need of accessing a mental patient's data in medical care against the patient's right to privacy. Two key considerations are whether the data being revealed include private conversations between the patient and psychotherapist, and if there are less invasive ways for the state to collect the required information.[xxxi]

Electronic Patient Record and Electronic Health Record – Patient Data Management

The landscape of confidentiality and privacy protection is evolving swiftly. The scenario where there is just one doctor, one patient, and one medical file is now obsolete.[xxxii] Medical institutions have implemented advanced record-keeping systems aided by information technology. By digitising patient data and integrating them with clinical decision-making systems, they become easily accessible to future healthcare practitioners. This allows for a comprehensive medical history of the patient to be instantly available, regardless of the time or location, facilitating informed healthcare choices. With the implementation of an electronic patient record system, physicians may conveniently get electronically accessible data from any location, regardless of whether it is inside or outside the same facility.[xxxiii]

The use of an electronic patient record offers clear and evident benefits. It provides diagnostic and therapeutic treatment that is focused on the needs of the patient. It mitigates the occurrence of duplicate laboratory and diagnostic tests, hence reducing potential harm to the patient and avoiding unnecessary use of valuable resources and time. An electronic patient record serves as a simple notification system for identifying incompatible prescriptions and bad responses to medications.[xxxiv] The efficacy of medical interventions may be evaluated. The electronic file enables the electronic access to medical standards and procedures, facilitating the selection of the most appropriate procedure based on the patient's condition. It enables individuals to have

control over their own actions, provides for independent verification and evaluation of novel technology and processes. Additionally, administrative operations are more efficiently executed compared to the process of handling patient files by hand. Overall, the use of contemporary information and communication technology in healthcare has significant potential for effectively fulfilling the right to receive healthcare, including providing accessible and high-quality patient-centered services.[xxxv]

Third parties are more likely to dispose of personal medical data collected for health care reasons as current communication and information technology makes it simpler to obtain. Medical data is rapidly outdated and sometimes inaccurate. To maintain the fiduciary relationship between patient and doctor, it is crucial to prevent improper disclosure of personal medical data, limit communication between health care providers to medically necessary data for the next treating physician, and obtain informed consent from patients before communicating outside of direct treatment. This relates to health care networks, where care services and cures flow smoothly.[xxxvi]

Patients need complete transparency in their digitised patient files. By recording medical file entries, modifications, and deletions, as well as access and communication, the patient should have simple data-flow visibility. Thus, the patient may manage his medical data, including his ability to change or delete it. Patients should have their rights maintained regardless of how medical data is gathered. Privacy protection should be determined by law, not technology. The doctor-patient relationship, including patient rights and doctor obligations, does not alter due to technology or health care service organisation. While the law remains the same, responsible use of ICT requires proper execution. Beware of computer screens interfering with doctor-patient relationships.[xxxvii]

Challenges in Electronic Patient Record

Additionally, there are many hazards associated with the use of electronic patient records. One of the significant disadvantages is the possible loss of the patient's rights to medical confidentiality and privacy. With the use of contemporary information and communication technology, personal medical data may be effortlessly sent and readily retrieved. The urgent

threat of inflation of the rules and principles established in international human rights treaties and state health legislation is inherent in this situation. If this potential threat becomes a reality, the electronic patient record has the potential to undermine the trust-based relationship between the patient and the doctor, rather than enhancing it.[xxxviii]

One first issue is the patients' autonomy in making choices as a component of their right to self-determination. Standardisation of medical language and concepts is essential for the electronic interchangeability of medical information. Healthcare decision-making may shift its focus from the individual patient to the information bundle. Under such circumstances, the patient's autonomy is compromised as they are no longer provided with alternate options to select from. This goes against the need of obtaining informed consent before any medical procedure. As per the Dutch "medical treatment agreement" statute, which outlines the rights of patients and responsibilities of physicians, doctors are obligated to educate patients about not just one potential course of action, but also about any other options and their expected consequences. Dutch doctors have been legally responsible for the lack of informed consent when they failed to notify the patient about alternative treatments. A lack of consent in this situation goes against the principles outlined in Article 8 of the European Convention on the protection of human rights and fundamental freedoms of the Council of Europe.[xxxix]

Another issue arises from the excessive accessibility and availability of personal medical information, including but not limited to - Medical records are always susceptible to unauthorised access. This issue is especially relevant when it comes to electronic patients' files. Therefore, in the event of electronically filing personal medical information, the use of privacy enhancing technology (PET) and access authorization mechanisms are crucial requirements. Additional relevant criteria include, for example, the limitation of data collection to just what is essential for the intended purpose, and the prompt disposal of medical information after its purpose has been fulfilled. To prevent creating a misleading picture of the patient by utilising obsolete medical information, it is necessary to comply with this criterion.[xl]

Further, due to the standardisation of electronic patient records, doctors have access to medical data that have been collected from many sources for the purpose of medical treatment. This access is not restricted to just the facts that are necessary for making treatment choices. The advent of the modern electronic information and communication system, which is inherently

open, poses a significant challenge for software designers to restrict permitted access to personal medical data only to the information that is actually required. The need of "necessity" is a crucial standard for safeguarding privacy, which must be maintained to ensure that patients do not lose trust in healthcare.[xli]

It is also well recognised that using a single personal identification number for many purposes leads to excessive data duplication. While the idea of using a single identifying number may sound appealing due to its simplicity, it does not seem to be necessary for the purposes of healthcare. To mitigate any adverse impacts, it is advisable to prioritise the implementation of a patient identity system that uses a distinct number for the healthcare industry, or alternatively, biometric identification technologies. These strategies will reduce the likelihood of patient data being accessed by interested third parties, such as employers and private insurance firms, hence minimising the hazards associated with data-linkage.[xlii] Additionally, consent obtained after providing all relevant information and ensuring the individual fully understands the implications and consequences is very crucial. The bigger the number of options available for data transmission, the higher the likelihood that the necessity for informed consent when transferring medical data to a physician not directly engaged in the continuing treatment may be overlooked. Doctors must be informed that privacy regulations dictate that the doctor and patient must reach a consensus on which data may be shared with whom and at what specific time.[xliii]

Confidentiality - Not Absolute

The idea of confidentiality helps patients feel comfortable providing all medical information. Such information helps the doctor diagnose accurately. It helps the doctor provide the patient with the best suitable treatment. Therefore, when a doctor takes a patient, they are expected to keep that specific information discreet and utilise it for the patient's advantage. The doctor cannot share patient medical information without consent.[xliv]

Nevertheless, there are several instances that deviate from this principle, like as Health insurance issues arise when private information is involved in a lawsuit or when physicians disclose medical information to others and classify it as a case study. However, in the event

that this data is disclosed in reputable scholarly publications, the patient's name remains confidential, and the patient has the legal entitlement to initiate legal action if their identify is disclosed in any manner.[xlv] Even in case where the concerned patient happens to be of minor age, the doctor is open to disclose the sensitive medical information to the minor patient's parents or guardians as the case be.

Indian Regulatory framework

At this juncture, it is paramount to be aware that as on today, there is no particular statute or any enactment in India, governing the concept of confidentiality between the Doctor-Patient Relationship even though it is a matter of most sensitive and private information of an individual which is connected with right of life of every citizen of India, being a fundamental right. However, there are few guidelines which every doctor or medical practitioner needs to follow.

According to chapter 7- (7.14) of the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Rules, 2002[xlvi], a licenced medical practitioner is prohibited from disclosing any patient information acquired during the provision of treatment or via the exercise of professional judgement. The consequences of the breach are examined in Chapter 8.2 of the regulations, i.e. if a complaint is made regarding the professional misconduct of a registered medical practitioner, the relevant medical council will conduct an inquiry. The said inquiry will be brought before the Medical Council of Disciplinary Action. The registered medical practitioner will be given reasonable opportunity of being heard in order to present their case in person or through a representative after receiving the complaint.[xlvii] If it is discovered that the registered medical practitioner has committed professional misconduct during the inquiry or legal process, if such a situation arises, the Medical Council will administer appropriate disciplinary measures, which may include the possibility of revoking his licence.[xlviii]

That apart, there are no such specific laws in India which protect the privacy and confidentiality of the patient's sensitive medical data but the Health Ministry has proposed a Digital Information Security in Healthcare Act (DISHA) in 2018 which has not been enforced though. Details of this proposed act shall be explained in the subsequent section.

Digital Information Security in Healthcare Bill (DISHA)

The Digital Information Security in Healthcare Act[xlix] (DISHA) is a legislation that aims to establish National and State eHealth Authorities and Health Information Exchanges. It is important to understand that though the act hasn't been passed, its purpose is to standardise and regulate the processes involved in collecting, storing, transmitting, and using digital health data. The act also focuses on ensuring the reliability, data privacy, confidentiality, and security of digital health data, along with addressing other related matters.[l]

The proposed health information legislation aims to govern two categories of data: Digital Health Data (DHD) and the corresponding personally identifiable information (PII). If implemented, DISHA will oversee and control the creation, gathering, retrieval, retention, transfer, and utilisation of DHD (Digital Health Data) and its related Personally Identifiable Information (PII).[li]

The Digital Information Security in Healthcare Act (DISHA) of India aims to create a National Digital Health Authority and Health Information Exchanges. The possible bill aims to streamline electronic health data privacy, confidentiality, security, and standardisation. DISHA and HIPAA have several similarities. The information governed by DISHA is analogous to that of HIPAA, since both legislations oversee personal health data. DISHA categorises the data they oversee into two types: Digital Health Data (DHD) and personally identifiable information (PII) that is connected with it. On the other hand, HIPAA controls protected health information (PHI) and specifically focuses on PHI that is kept electronically.[lii] (ePHI).

Relevant Case Laws

Mr X v. Hospital Z, 1998[liii]

In order to make blood transfusion to someone, the said respondent collected a sample of the appellant's blood. But it so happened that, respondent found out that the appellant was HIV positive. Subsequently, the Healthcare authorities revealed the sensitive information about the appellant's health condition to his concerned family members which resulted in the annulment of marriage as well. in this case, court held that the doctor-patient relationship is not absolute

and that it can be breached for the larger interest, i.e. interest of the public health. Therefore, respondent was not found guilty. However, the court held appellant guilty under sections 269 and 270 of the Indian Criminal Code on basis of the fact that appellant was aware of his illness but still decided to get married.

Mr Surupsingh Hrya Naik v. State of Maharashtra, 2007[liv]

In the current case, Right to Information Act, 2005 was in conflict with The Medical Council Code of Ethics where the issue was pertaining to making the patient's health records available under RTI Act would eventually violate the right to privacy guaranteed under Article 21 of Indian Constitution to every citizen. However, Bombay High Court ruled that the Right to Information supersedes the Right to Privacy and Confidentiality.

Missing Link

The Puttaswamy judgement[lv] influenced the ultimate ruling on the Aadhar programme, determining that some provisions of the Aadhar statute were unlawful based on the proportionality test. Nevertheless, the court affirmed the constitutional legitimacy of the Aadhar programme in its whole. The main dispute in the case was about the possibility of widespread surveillance and the establishment of centralised databases for aggregated data. The court determined that the collection of Aadhar data did not have sufficient information to enable the creation of individual profiling, since it solely consisted of demographic and biometric data.[lvi] The court's examination of the matter was grounded on the principles of data processing as outlined in the EU General Data Protection Regulation (GDPR), which serves as Europe's legislation pertaining to data protection and privacy. The Aadhar programme was deemed to comply with the standards outlined in the General Data Protection Regulation (GDPR), including lawfulness, purpose restriction, data minimization, accuracy, storage limitation, and secrecy. In the Puttuswamy judgement, the court determined that the aggregation of information silos could result in profiling, which it deemed unconstitutional. Consequently, the court ruled that these silos must remain integrated and further stated that private parties are prohibited from accessing these silos or any Aadhar database. The prohibition of private parties accessing Aadhar databases was brief. The Aadhaar and Other

Laws (Amendment) Act, 2019 disregards the court's rulings that deemed private party access to the databases as unlawful. The legislation effectively perpetuates the practice of using ambiguous language regarding the choice between voluntary and involuntary actions.[lvii] The amendment grants recognition to the idea of offline verification as a voluntary approach, allowing individuals to bypass the Aadhar authentication systems using a UIDA QR system.[lviii] However, the amendment fails to address the Supreme Court's ruling on Aadhar, which mandated restrictions on private entities' ability to perform authentication. While some may argue that Section 57 of the AOLA was invalidated due to access through a contractual situation, it would contravene the proportionality test established by Justice Chandrachud and the purpose limitation of GDPR, which was explicitly raised as an objection to Section 57 in the Aadhar judgement. While the court determined that Aadhar does not have the capacity to create a widespread surveillance system, the concept of government-authorized surveillance is not novel, as demonstrated by the PUCL case. In this case, the definition of privacy expanded beyond physical boundaries to encompass personal communications, and guidelines were established to regulate the exercise of surveillance powers. India has previously established several monitoring initiatives, namely. The user mentions many systems related to network traffic analysis, crime tracking, lawful intercept and monitoring, and national intelligence. These systems include Network Traffic Analysis System (NETRA), Crime and Criminal Tracking Network System (CCTNS), Lawful Intercept and Monitoring Project (LIM), and National Intelligence Grid (NAT-GRID)[lix]. The Central Monitoring System (CMS) and the Crime and Criminal Tracking Network and Systems (CCTNS) are examples of such systems. The mentioned systems include the Central Monitoring System (CMS), Network Traffic Analysis System (NETRA), Lawful Intercept and Monitoring Project (LIM), and National Intelligence Grid (NAT-GRID). The AP Shah committee[lx] has criticised some of these projects for having a "unclear regulatory regime" that lacks transparency. These initiatives persist beyond the Puttuswamy period and continue to evolve with technical progress. Clearly, the government is able to circumvent both the Puttuswamy judgement and the Aadhar judgement, raising doubts about the effectiveness of the right to privacy as a basic right in the present Indian environment.[lxi]

Prior to examining a potential cause for the lack of effectiveness, it is essential to comprehend the significance of data privacy in the present socio-political and socio-economic context. The

revelation of personal preferences across several domains has been shown to have significant consequences. This is shown by the Cambridge Analytica incident, which revealed that voter data may be used as a means of influencing elections.[lxii] In the greatest democracy on Earth, the capacity for extracting and analysing data is boundless, whether it is done by government entities or non-government entities. As a consequence, the importance of privacy extends beyond individual concerns. An emerging privacy issue pertains to the Indian Government's latest stance on Virtual Private Networks (VPNs). The Indian Computer Emergency Response Team has issued directives under the IT Act mandating that firms providing virtual private networks (VPNs) must retain and safeguard various consumer data, including contact details and IP addresses.[lxiii] Initially, it was said that corporate VPN service providers would need to keep client logs. However, it was subsequently clarified that this requirement would not apply to them. Considering that the primary purpose of a VPN is to ensure user anonymity by implementing "no logs" policies and other privacy-focused methods, the new CERT rules, which would be applicable to all VPN providers with servers in India, contradict the principle of privacy and do not seem to prioritise user privacy.[lxiv]

Due to this, some leading VPN providers have been refusing to adhere to the regulations that are scheduled to take effect by the end of June. Presently, some countries that impose strict regulations or completely prohibit the use of VPNs include China, North Korea, Russia, and several Middle Eastern nations. None of these governments have been known for upholding privacy rights. Regrettably, India seems to be deviating from the concept of safeguarding privacy that the court had envisioned, as a result of the enforcement of these new regulations.[lxv]

This leads us to a crucial concern about the implementation of privacy as a basic right in India: the insufficiency of appropriate laws.[lxvi] "Case law is a valuable resource, like gold in a mine, where only a few pieces of the precious metal are found among tonnes of useless material. On the other hand, statute law is like the currency of the country, readily available for immediate use." The remarks of John Salmond significantly align with the present status of privacy in India. The inclusion of privacy as a constitutional right in India was a necessary measure in response to the rise of big data. However, at present, any concerns regarding privacy can only be addressed through a writ petition, unless they fall within the limited scope of certain legislations, such as sections of the Information Technology Act or the Indian Penal Code,

which were not originally designed to address privacy issues.[lxvii] This results in a slower and more careful approach to meeting the requirements of the general public, which may be advantageous for both government organisations and commercial organisations, since they have more resources to engage in these legal disputes. Although the basic right to privacy aims to bring about social change, it is not completely successful in doing so. It might be argued that there is still work to be done, and legislation is needed to adequately recognise and safeguard this new fundamental right.[lxviii]

Further, based on Justice B N Sri Krishna committee's suggestions and recommendations, Personal Data Protection Bill was introduced which subsequently took the shape of Digital Personal Data Protection Act, 2023 in pursuance of the Puttuswamy judgment which plays a pivotal role in data protection.[lxix]

Digital Personal Data Protection Act, 2023

India has seen rapid digitalization in recent years. Therefore, the government is progressively recognising the need of regulating data in the nation, particularly personal and confidential data of every citizen. Digital Personal Data Protection Act was passed on 11th Aug, 2023 and came into force from 1st Jan, 2024. The legislation is expected to tackle privacy issues, mitigate cyber security dangers, and foster trust between companies and their consumers. The legislation would establish transparency and accountability measures for organisations that gather data, ensuring that these organisations are aware of their responsibility for the data they acquire from individuals. The DPDP Act, 2023 is said to replace India's existing patchwork of data protection rules.[lxx]

It is evident that the DPDP Act, 2023 has its roots in the EU's General Data Protection Regulation (GDPR) for removing ambiguity, providing transparency, accountability measures and especially while defining certain terminologies like 'personal data'[lxxi] 'Data Fiduciary'[lxxii] 'Data Processor'[lxxiii] & 'Data Principal'.[lxxiv] This apart, The origins of the DPDP Act may be traced back to the early 2000s. India started its foray into cybersecurity legislation with the enactment of the Information Technology Act of 2000. As technology advanced and the volume of digital data grew, it became clear that a more complete framework for protecting

data was needed. In the significant Puttaswamy case, India reaffirmed the significance of privacy by recognising it as a basic right under the Indian Constitution. This decision facilitated the implementation of stricter laws specifically targeting the safeguarding of data.[lxxv]

The DPDP Act imposes extensive obligations on the Data Fiduciaries and grants a set of entitlements to persons whose personal data is collected and used. These entitlements include the right to receive notification from the Data Fiduciary about the purpose for which their data is being used, as communicated via a notice. The entitlement to get information and the entitlement to have their data eradicated. The duties introduced pertain to restricting the purposes for which data may be used and the subsequent need to delete the data after its intended purpose has been achieved. The DPDP Act also creates a regulatory agency called the Data Protection Board of India (Board). The power of this Board includes the investigation of complaints and the imposition of sanctions.[lxxvi] The DPDP Act's primary highlights are as follows:

i. Scope and Application of the DPDP Act

The DPDP Act is be applicable to the processing of any personal data that is in digital format or has been subsequently digitised on a future date. This will include the handling of any data pertaining to any Indian citizen, with the processing occurring in a foreign country.[lxxvii] This explanation is crucial to prevent any exploitation of personal data of Indian citizens. Data 'processing' refers to the automated or partially automated actions performed on digital personal data. These actions include collecting, recording, organising, structuring, storing, adapting, retrieving, using, aligning or combining, indexing, sharing, transmitting, disseminating, restricting, erasing, or destroying the data.[lxxviii] The legislation would include processing activities conducted for commercial objectives, explicitly excluding data processing carried out by individuals for personal or domestic reasons, as stated in the DPDP Act. The DPDP Act has included an additional intriguing provision which stipulates that any information disclosed by its owner to the public shall be exempt from the scope of this DPDP Act.[lxxix]

ii. Data Fiduciaries And Their Obligations

A 'Data Fiduciary' refers to any organisation or individual within India that is entrusted with the ownership and management of personal data by a citizen, who is referred to as the 'Data Principal', with their explicit agreement.[lxxx] According to the DPDP Act, the Data Fiduciary will have authority over the methods of processing and the intended purpose of the processing. Section 5[lxxxi] of the DPDP Act discusses the concept of 'Notice', which is derived from the General Data Protection Regulation (GDPR) implemented in the European Union. Displaying a notification at all step of an online transaction where personal data will be gathered is a crucial responsibility of the Data Fiduciary.[lxxxii] The Notice will provide the Data Principal with details on the kind of information being gathered and the specific purpose for its collection. The objective must be legal and not prohibited by any legislation. Consent is a crucial responsibility of the Data Fiduciary, as stated in section 6[lxxxiii] of the DPDP Act. According to this section, the consent provided by the Data Principal must meet certain criteria. It should be freely given, specific, informed, unconditional, and unambiguous. Additionally, it should involve a clear affirmative action and indicate an agreement to process the individual's personal data for a specific purpose.[lxxxiv] The consent should also be limited to the personal data that is necessary for that specified purpose. This is a very cohesive subordinate clause about consent. According to the clause, the need for obtaining permission must be given clearly and comprehensibly in English or any other language listed in the eighth schedule of the constitution.[lxxxv] Simultaneously, all Data Principals own the right to revoke their permission at any given moment, and this revocation must be as effortless as the initial granting of consent.[lxxxvi] When permission is revoked, the Data Fiduciary will no longer have authority over the data and must notify its 'Data Processor', who handles the data on behalf of the Fiduciary, to stop processing the data.

iii. Data Principals And Their Rights

The DPDP Act delineates a precise set of entitlements for individuals whose data is being processed, which is more limited in extent when contrasted with the more expansive entitlements delineated in the GDPR.[lxxxvii] The DPDP Act guarantees people' rights, including the right to access, the right to have their data amended or deleted, and the right to receive prior notice before granting permission. As a result, specific rights such as the right to transfer data,

the right to object to processing for grounds outside permission, the right to have personal information erased, and the right to prevent decisions made solely by automated systems are not present.[lxxxviii] The legislation creates two distinct rights. The right to 'grievance redressal'[lxxxix] refers to the provision of a convenient contact point by the Data Fiduciary to address complaints from the Data Principal. The right to 'appoint a nominee'[xc] allows the data principal to designate someone who can advocate for their rights in case they are unable to do so due to death or incapacity.

iv. Exemptions

Section 17 of the DPDP Act has many exclusions including but not limited to specific situations from its application on cases where data processing is carried out to enforce a legal right or claim, personal data processing by courts, tribunals, or other authorised bodies in India responsible for judicial, quasi-judicial, regulatory, or supervisory functions, and processing necessary for the amalgamation, merger, arrangement, or reconstruction of two or more companies. Start-ups are given a specific exemption under section 17(3) which states that the Central Government can notify certain Data Fiduciaries, including start-ups, who are not required to comply with the provisions of section 5, sub-sections (3) and (7) of section 8, and sections 10 and 11, based on the volume and nature of personal data processed.[xci]

v. Data Protection Board

The Board has the authority to receive and examine complaints filed by Data Principals. However, this can only happen if the principal has completed the internal process for resolving complaints set up by the applicable Data Fiduciaries.[xcii] The Board has the authority to issue legally enforceable directives against people or businesses that break the law.[xciii] Additionally, it has the power to promptly enforce measures to correct a data breach. This include the implementation of monetary penalties and the authority to guide parties towards ADR (Alternate Dispute Redressal) processes. While the Board has been granted powers that are equal to those of a civil court, such as the ability to summon persons, admit evidence, and examine documents, the DPDP Act specifically prohibits the use of civil courts to apply its requirements.[xciv] This imposes a practical limitation on an efficient legal solution, similar to the remedy provided by Article 82 of the GDPR.[xcv] The DPDP Act allows anyone who have

been impacted by a decision issued by the Board the chance to submit an appeal to an Appellate Tribunal. This Tribunal is specifically designated as the Telecom Disputes Settlement and Appellate Tribunal, which was formed under separate law in India.[xcvi]

Digital Personal Data Protection Act, 2023 Impact on Healthcare Data Management

The introduction of the DPDP Act will provide people augmented rights and safeguards for their health data, enabling them to exercise their entitlement to access, rectify, and delete their health information.[xcvii] The DPDP Act emphasises the significance of ensuring the privacy and security of personal data across many businesses. In the healthcare industry, the implementation of digital technology is transforming the way hospitals and healthcare institutions handle and retrieve medical records to improve patient care. The DPDP Act is anticipated to redefine approaches for protecting data, maintaining patient privacy, and advancing medical capabilities. The DPDP Act specifically puts significant responsibilities on data fiduciaries and requires strict procedures to maintain the confidentiality and integrity of health data, with severe penalties for any breaches or security failures. This highlights the crucial need for strong cybersecurity standards.[xcviii]

Due to the implementation of the DPDP Act, data discovery has become an essential need in the healthcare industry. Healthcare organisations collect a significant amount of sensitive personal data, including information on children and adults with disabilities, from the time a patient is hospitalised until they are discharged.[xcix] The data is regularly shared with third-party suppliers, insurers, and digital healthcare organisations and platforms for numerous objectives, including making decisions based on data. However, in several cases, the storage and processing of this data lack adequate regulation and structured organisation. Moreover, the degree of digitalization in healthcare organisations in India fluctuates based on the scale of their activities. In light of these situations, it is essential for organisations to adopt a sustainable approach to data discovery in order to ensure strong data governance. Furthermore, the automation of this process is essential for ensuring sustainability.[c]

In order to improve data governance, healthcare organisations need to build a thorough framework for managing third-party data privacy. This framework should include a collection

of fundamental guidelines, resources, and methodologies designed to identify and mitigate risks while implementing efficient risk management procedures.[ci]

Few healthcare organisations have fully implemented security policies, standards, and procedures, although most have partially accepted them or are in development. Several healthcare industries require urgent cybersecurity upgrades. When installing or changing systems, design and configuration standards are essential.[cii] Most companies don't have centralised security monitoring. To secure data, healthcare firms should concentrate centralised active security monitoring, threat detection, incident response, vulnerability screening, and patching. When strengthening infrastructure, institutions should consider cloud-based security solutions.[ciii]

Secure on-site and remote access for physicians and privileged users has improved in healthcare. Multi-factor authentication (MFA) is an effective way to verify users' access to EHRs, patient data, and other vital systems. The added security layer improves security. This protects against internal attacks and credential risks.[civ]

In addition to solid security, organisations must frequently conduct privacy risk assessments on their technical systems. This requires assessing third-party risks throughout the supply chain, including suppliers, vendors, and service providers. Regulators should consider requiring manufacturers to design and secure medical devices. Additionally, post-installation cybersecurity vulnerabilities must be addressed.[cv]

As required by the DPDP Act, Indian healthcare companies should hire Data Protection Officers (DPOs) to oversee and ensure data protection compliance. These mitigating measures may take four to six months to execute, depending on the healthcare organization's size and infrastructure. Organisations must also fund process and structural development.[cvi]

Conclusion

In general, a doctor has a moral and professional obligation to keep patient information secret, unless there are specific legal restrictions. Doctor-patient confidentiality does not automatically

have legal protection in court proceedings, unless it is deemed that excluding such information would be in the best interest of the public.[cvii]

Confidentiality is crucial in establishing and maintaining trust in the doctor-patient relationship. An individual's therapy is contingent upon secrecy, with the level of trust determining the extent to which they may disclose their condition to their doctor. Ensuring privacy should be the highest concern in the Doctor-Patient Relationship. The technical avenues of computerised record keeping are growing rapidly. As a result, third parties' requests for personal information are likewise growing swiftly and in an unpredictable manner. In order to provide sufficient safeguarding of medical data privacy in today's times, it is necessary to take decisive measures at levels.[cviii]

Legislation should include initiatives to promote public knowledge of the issues and encourage community participation in finding solutions. Patients must be given an explicit entitlement to access any personal information created during their medical treatment, regardless of the context in which the information is used. It is important to ensure that the average individual can easily find and rectify any such information.[cix] The responsibility for notifying corrections should be assigned to the hospital and other organisations that are most capable of distributing such notifications and benefiting from the information. A legislation of this kind must mandate the presence of public, local proof to demonstrate compliance, as well as the provision of first public, local notice for the establishment or alteration of any computerised medical record system. Furthermore, the Act should include provisions for educational programmes aimed at hospital workers to instil an understanding of the issue and to eradicate negligent information practices. Ultimately, legislation should enforce rigorous security protocols on data systems and establish clear expectations for the conduct of staff members in medical data processing centres.[cx]

However, in India, the only regulations that govern this connection and secrecy are the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations of 2002. There is currently no legislation in place to safeguard the right to patient confidentiality. There are loopholes that need to be filled. For instance, the Right to Information takes precedence over the Right to Confidentiality, allowing anybody to access information via the Right to Information Act.

Ultimately, the changing regulations on confidentiality and data privacy in India's healthcare industry demonstrate the intricate relationship between personal rights, public health priorities, and technological progress. Although the Indian Medical Council Rules provide some structure for protecting patient information, the lack of explicit laws highlights the need for complete legislation.

Further, the proposed DISHA Bill seeks to rectify this discrepancy by establishing uniform protocols for the gathering, retention, and use of digital health information, with a particular emphasis on safeguarding privacy and ensuring security. Nevertheless, the implementation of the law is still waiting, which creates a considerable amount of ambiguity and risk in the way data is managed.

The Puttaswamy judgement and following legislative efforts, such as the DPDP Act, signify substantial progress in bolstering data protection and privacy rights in India. The DPDP Act provides strict responsibilities for data fiduciaries and seeks to guarantee openness, accountability, and individual rights in data processing.

Nevertheless, the successful execution of these laws requires collaborative endeavours from healthcare institutions, lawmakers, and regulatory agencies. Strong cybersecurity measures, comprehensive data governance frameworks, and strict compliance processes are necessary to successfully reduce risks and protect patient information.

Lastly, India must prioritise safeguarding sensitive health data while promoting innovation and enhancing patient care as it embraces digital transformation in the healthcare industry. To successfully navigate the changing environment of confidentiality and data privacy in healthcare, it is essential to be vigilant, take proactive actions, and collaborate with stakeholders.

Endnotes

[i] Kant, P., Law on Consent and Confidentiality in India, Legal Service India (2019) https://www.legalserviceindia.com/legal/article-6973-law-on-consent-and-confidentiality-in-india.html
[ii] Therapist Kamna Chhibber, head of department, Mental Health and Behavioral Sciences, Fortis Memorial Research Institute, Gurugram.
[iii] New York enacted the first statutory physician-patient privilege in 1828, et al. Dina Khajezadeh, Patient Confidentiality Statutes in Medicare and Medicaid Fraud Investigations, 13 AM. J.L. & MED. 105 (1987).
[iv] Ibid. § 98, at 244; see Comment, Privacy in Medical Information : A Diagnosis,33 U. FLA.L. REv. 394, 396 (1981) (citing C. DEWITr, PRIVILEGED COMMUNICATIONS BErWEN PHYSICIAN
AND PATIENT 13 (1958)).
[v] Comment, Public Health Protection and the Privacy of Medical Records, 16 HARV. C.R.-C.L.
L. REv. 265, 266 (1981). Common law survives in England, though a physician may request the court to keep his or her professional secrets confidential. E. HAr, MEDICOLEGAL AsPECTs OF HOSPITAL RECORDS 79-80 (2d ed. 1977). The physician, however, does not violate medical ethics if the law or the courts compel disclosure of a patient's confidential communications. Id. at 80. As stated by Lord Mansfield: If a surgeon was voluntarily to reveal [professional confidences] ... he would be guilty of a breach of honor and of great indiscretion; but to give that information in a court of justice, which by the law of the land he is bound to do, will never be imputed to him as any indiscretion whatever.
McCoRMICK ON EVIDENCE § 98, at 243 n.1 (Cleary 3d ed. 1984) (quoting The Duchess of Kingston's Trial, 20 How. St. Trials (1776)).
[vi]Encyclopedia of Surgery Editorial Team. (2021). Patient Confidentiality. In Surgery Encyclopedia. https://www.surgeryencyclopedia.com/Pa-St/Patient-Confidentiality.html

[vii] Ibid.
[viii] Supra note 5, ALA. CODE § § 15-23-11, 34-26-2 (1975); ALASKA STAT. § 08.86.200 (1987); ARK. R. EvID. 503 (1987); CAL. EvID CODE §§ 990-1007 (West 1988); COLO. REV. STAT. § 13-90- 107(1)(d)(1987); D.C. CODE ANN. § 14-307 (1987) HAW. R. EVID. 504 (1985); IDAHO CODE § 9-203 (Supp. 1987); IND. CODE § 34-1-14-5 (1986); IOWA CODE ANN. § 622.10 (West Supp. 1988); KAN, STAT. ANN. § 60-427 (1983); LA. REV. STAT. ANN. § 13:3734 (West Supp. 1988); ME. R. EVID. 503 (1987); MICH. COMP. LAWS ANN. § 600.2157 (1986); MINN. STAT. § 595.02
(Supp. 1988); MIss. CODE ANN. § 13-1-21 (Supp. 1987); Mo. REV. STAT. § 491.060 (Supp. 1988); MONT. CODE ANN. § 26-1-805 (1987); NEB. REV. STAT. § 27-504 (1985); NEV. REV. STAT. § 49.215 (1986); N.H. REV. STAT. ANN. § 329:26 (Supp. 1987); N.Y. CIv. PRAC. L. & R. § 4504 (McKinney Supp. 1987); N.C. GEN. STAT. §8-53 (1986); N.D. R. EvID. 503 (Supp. 1987); OHIO REV. CODE ANN. § 2317.02 (Anderson Supp. 1987); OK.LA. STAT. tit. 12 § 2503 (Supp. 1988); OR. REv. STAT. § 40.235 (1987); PA. STAT. ANN. tit. 42 § 5929 (1982); S.D. CODIFIED LAwS ANN. § 19-13-6 to 19-13-11 (1987); UTAH CODE ANN. § 78-24-8 (1987); VA. CODE ANN. § 8.01-399 (1989); WIS. STAT. § 905.04 (Supp. 1987);. Wyo. STAT. § 1-12-101 (1977).
[ix] Ibid. at 266, 272.
[x] Confidentiality of Patient Health Information, 56 J.A.M.A. 4 (Dec. 1985) (a position statement of the American Medical Record Association); see also McCOmiICK, supra note 55 §98 at 244.
[xi] Ibid.
[xii] Supra note 5, at 274-76.
[xiii] MCCORMICK, supra note 5, at 244.
[xiv] Morgan, Forewordto MODEL CODE OF EVIDENCE 28 (1942), quoted in MCCORMICK, supra note 5, at 244.
[xv] MCCORMICK, supra note 5.
[xvi] Supra note 5 et al Dina Khajezadeh, Patient Confidentiality Statutes in Medicare and Medicaid Fraud Investigations, 13 AM. J.L. & MED. 105 (1987).
[xvii] 542 F.2d 1064 (9th Cir. 1976) (acknowledging a nonabsolute constitutional right of privacy with respect to psychotherapist-patient communications cited in MCCORMICK, supra note 55 § 98, at 244; Hawaii Psychiatric Soc'y v. Ariyoshi, 481 F. Supp. 1028, 1039 (D. Hawaii 1979) (upholding a constitutionally protected right of privacy extending "to an individual's liberty to make decisions regarding psychiatric care without unjustified governmental inter- ference"); United States ex rel. Edney v. Smith, 425 F. Supp. 1038 (E.D.N.Y. 1976) (implying

its acceptance of the constitutional status of the psychotherapist-patient privilege), aff'dsub nom. Edney v. Smith, 556 F.2d 556 (2nd Cir.), cert denied, 431 U.S. 958 (1977); In re "B," 482 Pa. 471, 394 A.2d 419 (1978) (plurality opinion) (recognizing a constitutional right of privacy protecting psychotherapist-patient records); In re Lifschutz, 2 Cal. 3d 415, 467 P.2d 557, 85 Cal. Rpts. 829 (1970) (recognizing that psychotherapist-patient communications are included within the constitutional right of privacy, but that this protection is not absolute).

[xviii] McCoRMCi, supra note 5 at 244 (citing Lora v. Board of Educ. of N.Y., 74 F.R.D.565 (E.D.N.Y. 1977)).

[xix] Goldberg, In New York, the privilege has "been the object of nearly unaminous scholarly criticism." Lora, 74 F.R.D. 565, 574 (E.D.N.Y. 1977).

[xx] Ibid.

[xxi] Ibid.

[xxii] Forty-three states and the District of Columbia have enacted some type of psychotherapist-patient privilege: ALA. CODE § 34-26-2 (1987); ALASKA STAT. §03.35.030 (1985).

[xxiii] Arena v. Saphier, 201 N.J. Super. 79, 86, 492 A.2d 1020, 1024 App. Div. (1985).; These statutes vary in scope and application and many contain significant exceptions, et al ibid.

[xxiv] Taylor v. United States, 222 F.2d 398, 401 (D.C. Cir. 1955), quoted in Arena v. Saphier, 201 N.J. Super. 79, 86, 492 A.2d 1020, 1024 (1985).

[xxv] Ibid.

[xxvi] Dina Khajezadeh, Patient Confidentiality Statutes in Medicare and Medicaid Fraud Investigations, 13 AM. J.L. & MED. 105 (1987).

[xxvii] United States ex rel. Edney v. Smith, 425 F. Supp. 1038, 1043 (E.D.N.Y. 1976), aftd, 556 F.2d 556 (2d Cir. 1977), cited in Recent Developments,

[xxviii] Report No. 45, Group For the Advancement of Psychiatry,

[xxix] Comment, Evidence-The Psychotherapist-Patient Privilege-The Sixth Circuit Does the Decent Thing: In re Zuniga, 33 U. KAN. L. Rav. 385, 401 (1985). 1"ld. at 392.

[xxx] ' Sloan & Hall, Confidentiality of PsychotherapeuticRecords, 5 J. LGAL MwD. 435, 458 (1984).

[xxxi] Hawaii Psychiatric Soc'y v. Ariyoshi, 481 F. Supp. 1028 D. Hawaii (1979).

[xxxii] Henriette Roscam Abbing, Medical Confidentiality and Electronic Patient Files, 19 MED. & L. 107 (2000).

[xxxiii] Ibid.

[xxxiv] Ibid.

[xxxv] Ibid.

[xxxvi] Ibid at 104.

[xxxvii] Ibid.

[xxxviii] Ibid at 119.

[xxxix] Ibid.

[xl] Ibid.

[xli] Ibid at 110.

[xlii] Ibid.

[xliii] Ibid.

[xliv] Sumasri, Understanding Doctor-Patient Confidentiality Laws in India, MEDBOTS, (Mar 17th, 2023), https://medbots.in/blog/understanding-doctorpatient-confidentiality-laws-in-india

[xlv] FindLaw. (2021). Breaches of Doctor-Patient Confidentiality. FindLaw. https://www.findlaw.com/injury/medical-malpractice/breaches-of-doctor-patient-confidentiality.html.

[xlvi] Indian Medical Council (Professional Conduct, Etiquette And Ethics) Regulations, 2002 governing the acts of every registered medical practitioner.

[xlvii] Henriette Roscam Abbing, Medical Confidentiality and Electronic Patient Files, 19 MED. & L. 107 (2000).

[xlviii] Ibid.

[xlix] Compliancy group, https://compliancy-group.com/disha-and-hipaa-how-do-they-compare/

[l] Ibid.

[li] Ibid.

[lii] Ibid.

[liii] Gupta, Y. vs. Hospital Z. Indian Legal Solutions. indianlegalsolution.com/mr-x-vs-hospital-z/.

[liv] Chaturvedi, S., Srinivas, K., & Muthuswamy, V. (2016). Biobanking and Privacy in India. Journal of Law, Medicine & Ethics, 44(1), 45-57. 10.1177/1073110516644198

[lv] Justice K. S. Puttaswamy (Retired.) and another. v Union of India and others, (2017) 1 SCC 10.

[lvi] Advait Kandiyoor, The Recognition of the Right to Privacy and Its Translation into Data Protection Laws in India, 4 INDIAN J.L. & LEGAL RSCH. 1 (2022).

[lvii] Raghu, Six Reasons Why the Aadhaar Amendment Ordinance Undermines Democracy, The Wire, Mar 12th, 2019.
[lviii] Indian Penal Code, 1860, Section 378, 379.
[lix] Akshi Gill & Aditi Jaiswal, DATA SURVEILLANCE: NEED FOR A POLICY TO ACHIEVE EQUILIBRIUM BETWEEN STATE AND INDIVIDUAL INTEREST, 8 Nirma University Law Journal, 57 (2018).
[lx] Planning Commission of India, Report of the Group of Experts on Privacy, 7: 19, p. 60-61, Oct 16 2012.
[lxi] Supra note 58.
[lxii] Adrian Chen, Cambridge Analytica and our Lives Inside the Surveillance Machine, The New Yorker Mar 21st 2018.
[lxiii] Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Govt. of India, No. 20(3)/2022-CERT-In.
[lxiv] Ibid.
[lxv] Tech Desk, The Indian Express, Express VPN, SurfShark shuts down India servers: Here's everything that happened so far, June 8th 2020.
[lxvi] Supra note 58.
[lxvii] Ibid.
[lxviii] Ibid.
[lxix] Supra note 55.
[lxx] Indian's existing data protection rules consisting of but not limited to Section 43A and 87(2)(ob) of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[lxxi] Digital Personal Data Protection Act, 2023, s 2(t).
[lxxii] Digital Personal Data Protection Act, 2023, s 2(i).
[lxxiii] Digital Personal Data Protection Act, 2023, s 2(k).
[lxxiv] Digital Personal Data Protection Act, 2023, s 2(j).
[lxxv] Cristina Pop, India's Digital Personal Data Protection Act: Key Provisions and Business Implications, Endpoint Protector (2023), https://www.endpointprotector.com/blog/indias-personal-data-protection-bill-what-we-know-so-far/
[lxxvi] Kermina Minoo Patel, The 2023 Digital Personal Data Protection Act: Evaluating Its Strength in Protecting Citizen Data, 4 JUS CORPUS L.J. [234] (2023).
[lxxvii] Ibid.
[lxxviii] Digital Personal Data Protection Act, 2023, s 2(x).
[lxxix] Latham & Watkins, India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison, Latham & Watkins LLP, (2023), https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf
[lxxx] Supra note 308.
[lxxxi] Digital Personal Data Protection Act, 2023, s 5.
[lxxxii] Ibid.
[lxxxiii] Digital Personal Data Protection Act, 2023, s 6.
[lxxxiv] Tech Desk, The Indian Express, Express VPN, SurfShark shuts down India servers: Here's everything that happened so far, June 8th 2020.
[lxxxv] Akshi Gill & Aditi Jaiswal, DATA SURVEILLANCE: NEED FOR A POLICY TO ACHIEVE EQUILIBRIUM BETWEEN STATE AND INDIVIDUAL INTEREST, 8 Nirma University Law Journal, 57 (2018).
[lxxxvi] Ibid.
[lxxxvii] Ibid.
[lxxxviii] Blumenthal D, Tavenner M. The "meaningful use" regulation for electronic health records, 363(6) N Engl J Med, 501-504 (2010).
[lxxxix] Digital Personal Data Protection Act, 2023, s 13.
[xc] Digital Personal Data Protection Act, 2023, s 14.
[xci] Digital Personal Data Protection Act 2023, s 17(3).
[xcii] Kermina Minoo Patel, The 2023 Digital Personal Data Protection Act: Evaluating Its Strength in Protecting Citizen Data, 4 JUS CORPUS L.J. [234] (2023).
[xciii] Supra note 84.
[xciv] Ibid.

[xcv] General Data Protection Regulation 2016, art 82.
[xcvi] Supra note 84.
[xcvii] Anjan Bhattacharya, How the DPDP Act reshapes the healthcare sector's compliance requirements, FE healthcare (2023), https://www.financialexpress.com/healthcare/pharma-healthcare/how-the-dpdp-act-reshapes-the-healthcare-sectors-compliance-requirements/3275527/
[xcviii] Ibid.
[xcix] Pharmaways Global Private Limited, (2023), https://pharmaways.in/how-the-dpdp-act-reshapes-the-healthcare-sectors-compliance-requirements/
[c] Ibid.
[ci] Ibid.
[cii] Ibid.
[ciii] Digital Personal Data Protection Act, 2023, s 5.
[civ] Ibid.
[cv] Latham & Watkins, India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison, Latham & Watkins LLP, (2023), https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf
[cvi] Ibid.
[cvii] Jerome R. Morse & Anna L. Casemore, Doctor-Patient Confidentiality: To Disclose or Not to Disclose, 22 ADVOC. Q. 312 (2000).
[cviii] Aileen A Lee, Electronic Data Processing in Private Hospitals: Patient Privacy, Confidentiality and Control, 13 SUFFOLK U. L. Rev. 1386 (1979).
[cix] Dina Khajezadeh, Patient Confidentiality Statutes in Medicare and Medicaid Fraud Investigations, 13 AM. J.L. & MED. 105 (1987).
[cx] Aileen A Lee, Electronic Data Processing in Private Hospitals: Patient Privacy, Confidentiality and Control, 13 SUFFOLK U. L. Rev. 1386 (1979).