

Indian Privacy Laws and the Need for Reform in light of Artificial Intelligence

Ms. Mohita Yadav¹, Dr. Arti Sharma²

¹Ph.D Scholar, Jagannath University, Bahadurgarh, Haryana

²Head of the Department and Assistant Professor, Jagannath University, Bahadurgarh, Haryana.

Abstract

The rapid advancement of artificial intelligence (AI) has raised significant concerns regarding privacy and data protection in India. The country faces multiple challenges which are required to be addressed, for instance, Data Collection and Surveillance, Lack of Transparency and Accountability, Cross-border Data Flows and Consent and Data Ownership. The privacy landscape in India has been evolving, particularly in light of technological advancements like artificial intelligence (AI). India till 2023 did not have a comprehensive standalone privacy law but has seen a range of legislative and judicial actions along with constitutional provisions to protect individuals' privacy. While the right to privacy has been recognized as a fundamental right by the Indian Supreme Court, the existing legal framework, including the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023 (DPDP Act), remains inadequate to address the complex challenges posed by AI technologies. AI systems, which rely on vast amounts of personal data, raise critical issues related to data collection, surveillance, accountability, consent, and cross-border data flows. The lack of transparency in AI decision-making and the risks of biased or discriminatory outcomes further exacerbate privacy concerns. AI presents both opportunities and risks when it comes to privacy. While India has made progress in terms of privacy protections, there is a growing need to modernize the legal framework to ensure it effectively addresses the challenges posed by AI. This paper highlights the need for reform in India's privacy laws, advocating for stronger data protection mechanisms, greater accountability for AI systems, and enhanced digital literacy to ensure individuals can make informed choices regarding their data. A robust legal framework, incorporating AI-specific provisions, is essential for balancing technological progress with the protection of fundamental privacy rights. The paper calls for a re-evaluation of existing comprehensive and other laws and the introduction of ethical guidelines for AI to ensure that technology serves the interests of both individuals and society at large.

Keyword: Artificial Intelligence, DPDP Act 2023, Right to Privacy, Reforms, Data Collection and Surveillance

Introduction

The widespread application of artificial intelligence in the government sector has caused a major change in the healthcare industry in recent years. Given pressing issues like poverty, the ongoing epidemic, and barriers to healthcare access, this change is particularly apparent. The world is dealing with complicated problems, and as a result, the fields of government surveillance and digital health are expanding rapidly and gaining significance.

It is possible that the healthcare system in India has undergone a profound paradigm shift. Digital platforms are progressively replacing traditional in-person consultations as the primary means of contact between patients and physicians. The dynamics of healthcare service delivery and access have fundamentally changed as a result of this revolutionary movement. With its advantages in terms of accessibility, efficiency, and ease of use, the emergence of digital platforms is altering the traditional means of communication between patients and physicians. The advent of artificial intelligence (AI) in the healthcare sector has completely changed how medical data and information are managed.

The phrase "digital health" refers to a wide concept that involves forming a partnership between digital technologies and the healthcare industry to increase healthcare efficiency and give patients more individualised treatment. The *Digital Information Security in Healthcare Act of 2018 (DISHA)*¹ defines "digital health data" as offering an electronic record of a person's health-related information", even though the terms "digital health," "digital medicine," and "digital therapeutics" are not defined explicitly in India. Often, the term "said data" refers to relevant information regarding a person's physical and mental health, medical treatments received, biological material or body parts donated, and test and examination findings. Genetics and digital technologies for early disease detection and treatment best exemplify the concept of digital health.

Leading this digital healthcare revolution is the Ayushman Bharat Digital Mission, an enormous project that has made a name for itself as one of the world's biggest health databases. By creating over 243 million health accounts and IDs, this effort has accomplished a noteworthy milestone that highlights the scope and influence of digital activities inside the Indian healthcare system. Gaining a complete knowledge of the complexities and ramifications of a database this size is essential to comprehending the larger picture of India's progress in digital health.²

But for all the revolutionary promise of digital health, there is also a risk to personal freedom. Despite this encouraging trend, the comprehensive use of AI in healthcare faces privacy obstacles. The lack of qualified specialists is a significant barrier that leads to expensive mistakes, delayed development, and increased healthcare costs. As a result, tech businesses are increasingly relied upon by healthcare providers for their proficiency in deploying AI solutions. Because of the increased need for AI in healthcare data security, technology companies are competing more fiercely to provide innovative solutions and obtain a competitive advantage.

As regards Government Surveillance, the Indian government has been using facial recognition technology (FRT) more and more for surveillance, law enforcement, and administrative purposes. Officials argue that technology increases security and efficiency, but concerns about privacy, misuse, and oversight gaps persist. The Automated Facial Recognition System (AFRS) is used by the Indian government for a number of purposes, including crime prevention

¹ *Digital Information Security in Healthcare, Act (DISHA), 2018, Acts of Parliament, 2018 (India)*. Available at: <https://archive.org/details/draftdishaaact> (Accessed: 10th January, 2024)

² *Update on Digital Healthcare Mechanism (21st July 2023) Press Information Bureau*. Available at: <https://pib.gov.in/PressReleasePage.aspx?PRID=1941463> (Accessed: 5th December 2023).

and law enforcement. Police in Tamil Nadu, Telangana, Punjab, and Delhi have integrated FRT for law enforcement and criminal detection. FRT was deployed by Delhi Police during rallies, such as those against the CAA.

Rapid technological integration has exposed weaknesses, especially with regard to personal data given by patients. Such sensitive data can be exploited in ways that seriously compromise privacy; thus, strong legislative protections must be put in place. AI poses questions regarding patient privacy and data security of common people even as it presents previously unheard-of possibilities to enhance medical treatment and results. In order to protect privacy and data security, this study traverse the advantages, complexities, and potential solutions of Artificial Intelligence (AI) as it relates to healthcare data and government surveillance. In this article, we also explore the changing legal environment with particular attention to the artificial intelligence, IT Act of 2000³ and the DPDP Act of 2023⁴. The aim is to tackle these apprehensions and institute measures that maintain the digital era's right to privacy with growing use of AI.⁵

Artificial Intelligence in Healthcare Data Security⁶

Organisations are implementing numerous applications that store and exchange enormous volumes of patient data as a result of the advancements in healthcare technology. Sensitive records are more vulnerable to unauthorised access thanks to these applications, which are motivated by healthcare data security⁷. It is imperative to have a more comprehensive strategy for safeguarding healthcare data because of this heightened exposure. Medical history, diagnosis, and treatment plans are among the extremely private information found in patient records. These could have disastrous results if they end up in the wrong hands. These could result in identity theft, insurance fraud, or even interrupted health care if they end up in the wrong hands. In healthcare data security, artificial intelligence (AI) is essential for identifying and averting any risks. In order to provide a prompt response to any suspicious behaviour, advanced AI-driven security systems are able to proactively monitor data access and identify anomalies in real-time. Healthcare companies may guarantee adherence to stringent data protection laws and secure patient privacy by utilising AI.

Furthermore, because medical data is so valuable, fraudsters have made healthcare organisations their top target. Data breaches are more likely as a result of the proliferation of electronic health records (EHRs) and linked systems. Hackers frequently target healthcare organisations in an attempt to profit financially or to take advantage of weaknesses in these systems. AI in healthcare data security is crucial for this reason. To safeguard sensitive documents, it provides sophisticated encryption and automatic defences. In addition to

³ *The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India)*

⁴ *The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)*

⁵ Hiloidhary, M. and Deka, B., 2022. *Privacy and Data Protection in the Digital Era: Prospect & Challenges*. Issue 2 Indian JL & Legal Rsch., 4, p.1.

⁶ Henry, J. and Abeer, B., 2024. *Healthcare data security: protecting patient information in sustainable data stores*. EasyChair Preprint, (12212).

⁷ Rajawat, A.S., Bedi, P., Goyal, S.B., Shaw, R.N., Ghosh, A. and Aggarwal, S., 2022. *Ai and blockchain for healthcare data security in smart cities*. *AI and IoT for Smart City Applications*, pp.185-198.

protecting patient privacy, putting strong cyber-security protections in place also guarantees public confidence in the healthcare system.

There are numerous roles played by AI in healthcare sector. By improving diagnosis and treatment and enabling quicker and more accurate decision-making, artificial intelligence is revolutionising patient care, through machine learning and sophisticated algorithms. This feature makes it possible to create individualised treatment plans based on the unique characteristics of every patient and accelerates the identification of diseases like cancer or cardiovascular disorders. AI-powered diagnostic technologies are always developing, providing medical professionals with more in-depth knowledge and facilitating better patient outcomes. Healthcare apps are transforming the way that therapies are customised in the field of custom software development. AI-powered healthcare applications are able to provide highly personalised treatment regimens by analysing a patient's genetic information, medical history, and lifestyle data.

AI is significantly improving hospital operations and lowering administrative workloads in addition to providing direct patient care. Routine duties that might be laborious and error-prone, such as managing patient information, arranging appointments, and billing medical professionals, can place a heavy burden on hospitals.

Budgetary constraints frequently prevent smaller healthcare providers from investing in cutting-edge AI for healthcare data protection⁸. Due to a lack of resources, staff members may not receive the required data security training and critical software updates may be delayed. Smaller suppliers become easy targets for fraudsters in the absence of these efforts, who take advantage of antiquated technology and lax security measures. These organisations are exposed to ongoing threats since underfunded defences are frequently neglected.

One of the most common reasons for data breaches in the healthcare industry is human mistake. Even something as basic as an employee giving private medical information to the incorrect person by mistake might have disastrous results. Furthermore, there are serious hazards associated with insider threats, in which workers take advantage of their position to obtain financial stability.

For instance, an employee of a hospital once sold patient information to identity thieves. In order to lower these risks, such instances highlight the necessity of strict internal controls, employee awareness, and frequent training initiatives.

Serious patient privacy violations can result from data breaches in the healthcare industry. The biggest health insurers in the United States, Anthem Inc., suffered a breach in 2015 that resulted in the exposure of 78.8 million clients' personal information. Sensitive data, including Social Security numbers, was among the exposed data, highlighting the serious repercussions of

⁸ Yeng, P.K., Nweke, L.O., Woldaregay, A.Z., Yang, B. and Snekenes, E.A., 2021. *Data-driven and artificial intelligence (AI) approach for modelling and analyzing healthcare security practice: a systematic review. In Intelligent Systems and Applications: Proceedings of the 2020 Intelligent Systems Conference (IntelliSys) Volume 1 (pp. 1-18). Springer International Publishing.*

inadequate data security safeguards. Such violations can undermine confidence, have legal repercussions, and emphasise the importance of ongoing watchfulness.

Healthcare organisations are exposed to sophisticated assaults when they take a reactive strategy to cyber-security. Rather, taking preventative action can greatly bolster defences. By constantly scanning for risks, utilising AI in healthcare data security improves protection. It is crucial to take proactive measures to guarantee patient data security, provide access to only authorised staff, and rigorously restrict data usage to authorised reasons. This proactive approach reduces vulnerabilities before attackers take advantage of them, strengthening the cyber-security environment.

A composed and well-thought-out reaction is essential in the regrettable case of a data breach. Therefore, Healthcare organizations shall be bound by strict regulations like data protection laws, which mandate the protection of patient data. Non-compliance shall result in heavy penalties, as seen in cases where hospitals have been fined for legal violations.

AI and Government Surveillance in India: Using Face Recognition Technology for State Monitoring and Surveillance

Facial recognition, as the name implies, is an AI-based technology that maps facial traits from an image or video using biometrics. In order to protect user privacy and guarantee that only they can access the material on their device, Apple created Face ID in 2017. The same idea is still used by banks today, who provide facial recognition to their customers for increased security. It's even used by Facebook to anticipate photo tagging. So, is the distinction between privacy and innovation becoming blurred by facial recognition? People worry about increased surveillance as a result of this application's broad use, particularly in public areas. It is similar to being constantly observed on the "Big Brother" show. The issue of privacy always comes up, even if AI and facial recognition provide many advantages in terms of safety and wellbeing.

Facial Recognition Technology (FRT) has been used more and more by the Indian government for administrative, law enforcement, and surveillance functions. Although officials contend that technology improves efficiency and security, worries about privacy, abuse, and a lack of oversight still exist. The Indian government is using it for multiple purposes like Law Enforcement & Crime Prevention by Automated Facial Recognition System (AFRS). Delhi, Telangana, Punjab, and Tamil Nadu police have integrated FRT for crime detection and law enforcement. Delhi Police used FRT in protests (e.g., anti-CAA protests).

Other areas are like Public Surveillance & Smart City Projects where FRT-enabled CCTV cameras are placed in public spaces to monitor crowds, protests, and sensitive areas. They have been integrated into Smart Cities Mission for urban security and traffic monitoring. Border Security & Immigration where it is used by Immigration and Visa Services (IVFRT) to verify identities at airports and land borders and also deployed for monitoring illegal migration and cross-border threats. Aadhaar & Citizen Verification i.e. FRT being explored to enhance Aadhaar authentication and Airports (e.g., DigiYatra at Delhi, Bangalore) use FRT for seamless boarding.

When facial recognition was initially introduced, it was thought to be helpful but required a lot of human intervention. But things have altered significantly with the development of AI and machine learning. Capturing, combining, or analysing large amounts of facial feature photos via cameras, sensors, cellphones, and social media platforms is not difficult these days. Computer scientists can quickly and effectively build models of a person's appearance using the appropriate algorithm, even if the image is grainy or blurry. And to be honest, this is a significant discovery, but it worries us. Technology is developing quickly, and advancements in AI and facial recognition are growing more sophisticated each time. For more accuracy and precision, tech behemoths like Amazon, Facebook, Google, and Microsoft are aiming to improve their facial recognition algorithms. In order to facilitate quicker and more seamless facial image exchange, Dell and HP are also evaluating their next-generation server capabilities. Facial recognition algorithms have advanced more than 20 times between 2014 and 2018, according to the National Institute of Standards and Technology (NIST), USA. A noteworthy accomplishment is the 95% decrease in error rates⁹.

According to experts, the development of technology may result in its responsible acceptance and application. As an illustration, the Indian government has begun to make extensive use of this technology to improve its capacity for law enforcement. According to reports, they intend to develop an Automated Facial Recognition System (AFRS) that will be used nationwide to track and identify criminals.

Facial recognition is another crucial tool that the Delhi Police have been adopting to improve their operations. This program, created by INNEFU Labs in India, uses artificial intelligence (AI) to sort through a large data set and connect people with their personal information. After identifying and extracting faces from an image, the technique turns each image into a vector with 512 values. After that, the program determines the shortest path between two vectors in a selected database. The ultimate outcome is then determined by the closest matching.

Facial recognition has numerous advantages, including combating human trafficking, identifying criminals, guaranteeing public safety, and locating missing children. The success of Delhi Police in tracking down almost 3,000 missing children in just four days after implementing a new facial recognition system serves as an example. The algorithm compared and evaluated over 45,000 current photos of children in the city with older photos of missing children using a database called TrackChild. The Indian government's Ministry of Railways also intends to combat crime by using facial recognition technology. In Bengaluru, the system is being tested. Approximately half a million faces are scanned daily, and AI compares them to faces in a police database of criminals. Additionally, the Ministry intends to expand the use of facial recognition software on trains.

AI and facial recognition are being applied appropriately in a number of other situations. A group of scientists, programmers, designers, and vehicle enthusiasts called FishEyeBox¹⁰ is working to create AI for linked objects innovation. They work on everything from low level

⁹ Geetika Sachdev, "AI and Facial Recognition: A Double-Edged Sword?" (2020) <https://indiaai.gov.in/article/ai-and-facial-recognition-a-double-edged-sword> (last visited 29th January, 2025)

¹⁰ <https://in.linkedin.com/company/fisheyeboxindia>

driving firmware actuation for universal interoperability to high level driving behaviour modelling and robotic scene estimation.

Existing privacy concerns with surveillance

Human rights advocates, privacy watchdogs, and the legal community have issued misuse warnings in response to the growing use of facial recognition technology. Many point to China as an example, where everything is watched, including border control, speeding, jaywalking, and security monitoring. The nation has come under heavy fire for "spying" on its citizens, while being a leader in the adoption of high AI standards.

Because people feel like they are constantly being "watched on," San Francisco, in the United States, has outlawed the use of face recognition technology by law enforcement and other organisations. This public outrage has been caused by a number of issues in addition to these worries. People always worry about their data and photos being exploited, especially since there aren't any laws governing facial recognition technologies. Furthermore, it is concerning because it is less accurate and more biased, particularly when it comes to its use in law enforcement. Additionally, it may result in erroneous convictions and misidentifications, particularly if the technology has not been updated. When it comes to technology use, particularly in the context of the legal system, accuracy and accountability are crucial. Additionally, there is mistrust regarding the protection of data privacy and the possibility of losing crucial information in the event of a data breach.

Technology bans end up being ineffective since they suppress rather than promote public discourse. The purpose of AI and facial recognition technologies is to let us view ourselves via technology, not the other way around.

Legal Framework to protect privacy breaches due to AI

India's overall data protection framework is made up of the Intermediary Guidelines, the SPDI Rules¹¹, and the IT Act. Online transactions and electronic data transfers are secure because to the IT Act's improved security measures. The enactment of the IT Act in 2000 was crucial in forming India's legislative foundation for the digital age. At first, the main goals of the Act were to legalize electronic transactions and regulate electronic trade. Its provisions covered a wide range of topics, including the gathering, exchanging, and moving of private information. Nevertheless, its implementation in the nascent field of e-health, particularly with regard to the protection of private health data, was deemed inadequate. The Act lacks the requisite detail to adequately address the unique issues of patient confidentiality and the digitization of healthcare information.¹² The Information Technology Act, although revolutionary in its day, focused mostly on topics such as digital signatures, cybercrimes, and electronic transactions. Sensitive health information could not be sufficiently protected by the wide and imprecise data protection rules. A more complete legislative framework was necessary to meet the intricacies of personal health data security in the digital era, as the digital health sector grew. The swift expansion of

¹¹ Available at: <https://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf> (Accessed: 25th December, 2023)

¹² Choudhary, P., 2022. Digital Information Security and Privacy Protection in Healthcare Sector in India. Issue II, Indian JL & Legal Rsch., 4, p.1.

digital health platforms has highlighted the inadequate protection of health-related data provided under the Information Technology Act. There were restrictions on the Act's capacity to address the unique issues of e-health, such as patient confidentiality, safe medical record handling, and data breaches. A desire for legislation that could effectively regulate and secure the privacy of personal health information in the digital sphere evolved as a result of the realization that a specialized legal framework was required to meet the complexities of health data protection.

The way the digital world has changed, especially in the healthcare industry, has made it clear that we need a stronger, more comprehensive data protection regulation. The Information Technology Act was a major step forward, but it fell short in addressing the ever-changing issues brought on by the expansion of digital health platforms. It became necessary to pass specialized law that was designed to address the complexities of protecting personal health data in order to give consumers and healthcare professionals' confidence that their private information would be treated with the utmost security and privacy.¹³

After realizing that the current legal framework was out of date and that an updated legal framework was urgently needed, the Indian government introduced the DPDP Bill in 2019. In order to solve the shortcomings in data protection, especially the protection of personal health information, this act represented a revolutionary move. Acknowledging the particular problems presented by the digital era, the law sought to establish a comprehensive and systematic approach to the handling of personal data by the government, organizations, and individuals. The following passage of the law in 2023 demonstrated the dedication to improving data protection protocols in the dynamic world of digital health platforms, including strong protections for personal health information.¹⁴

The Digital Personal Data Protection Act, 2023 vis-à-vis DISHA

A turning point in India's legal system was reached with the passage of the DPDP Act, 2023, especially with regard to the protection of private health information online. After being formally ratified by the president on August 11, 2023, this law is a proactive reaction to the growing issues brought about by the fast development of digital health platforms. It also represents a critical step in strengthening the regulatory framework of the country. The Act's scope is broad and all-encompassing, extending beyond national borders to cover corporations operating both domestically and internationally, Indian people, and entities that are formed under Indian law. This wide application, which acknowledges the ubiquity of digital health platforms and the numerous players involved, is a calculated effort to guarantee that the safeguards for personal health data transcend particular industries.

After mostly focusing on electronic transactions and communication, *the Information Technology Act of 2000* was replaced by the *Digital Personal Data Protection Act of 2023*,

¹³ Tekchandani, K., 2023. *Health in the Digital Era: A near Future Not a Distant Dream*. *Supremo Amicus*, 23, p.395.

¹⁴ Thomas, S. and Ravindra, M., 2023. *Right to Privacy in the Digital Era*. *Issue I Indian JL & Legal Rsch.*, 5, p.1.

which represents a paradigm shift. The recently enacted legislation provides a comprehensive and nuanced framework for the security of personal health data, recognizing the unique issues present in the digital health ecosystem. The Information Technology Act established the framework, but the 2023 Act skilfully adjusts to the changing digital environment and takes into account the complexities of today's data protection issues. This legislative change demonstrates the government's steadfast dedication to keeping up with technology developments and making sure that there are strong legal safeguards in place to deal with new issues that arise in the digital age.¹⁵

Following the worldwide COVID-19 epidemic, a number of poor countries, most notably India, are about to experience a profound digital transformation. The government of India recognizes the need for cyber-security and has created strong rules to protect digital data in accordance with its Digital India Mission. The planned *Digital Information Security in Healthcare Act (DISHA)* is a critical step in this direction. The National Digital Health Authority, health information exchanges, privacy, security, and standardization of electronic health data are all addressed by this legislative project.¹⁶

Worldwide, multiple nations have put laws into place to safeguard personal health information. *The Health Insurance Portability and Accountability Act of 1996* in the US is one well-known instance. Patients now have a great deal of control over their protected health information thanks to this legislation, which creates a framework for privacy and health information protection. Comparably, health data is covered by the GDPR of the European Union, which is similar to DISHA's function in India.¹⁷

The Act of 2000 and the *IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011* now comprise the legal framework that governs e-health protection in India. This framework offers some security for the collecting, sharing, and transferring of private information, including health history. However, a number of issues remain unresolved as a result of the legislation's failure to keep up with the quick advances in technology.

The national government launched the Personal Data Protection Bill of 2019 and DISHA to close this gap. The latter covers the State, Indian businesses, Indian individuals, and entities established in accordance with Indian law when processing personal data within India. Additionally, it broadens its scope to include international businesses that handle personal data in relation to operations in India. Comprehensive regulation is becoming necessary as more clinical facilities and healthcare providers in India use Electronic Medical Records and Electronic Health Records. Every patient must have an Electronic Medical Record according

¹⁵ *Ibid.*

¹⁶ Luniya, V. et al. (2021) *Disha – India's probable response to the law on protection of Digital Health Data, Healthcare - Food, Drugs, Healthcare, Life Sciences - India*. Available at: <https://www.mondaq.com/india/healthcare/1059266/disha-india39s-probable-response-to-the-law-on-protection-of-digital-health-data> (Accessed: 25 November 2024).

¹⁷ *Ibid.*

to the *Clinical Establishments (Registration and Regulation) Act of 2010*, and the Ministry of Health and Family Welfare established EHR Standards in 2013 (which were updated in December 2016) to provide a standardized process for building and managing Electronic Health Records.¹⁸

Regulations governing the creation, gathering, access, storing, transfer, and utilisation of Digital Health Data and related individually identifiable information are included in DISHA. Health information is categorized as the sole property of the individual to whom it relates, including information about sexual orientation, physical and mental health issues, medical records, and biometric information. The formation of State Electronic Health Authorities (SeHA) and the National Electronic Health Authority (NeHA), which oversee healthcare facilities and companies that collect Digital Health Data, are important aspects. DISHA suggests severe consequences for anyone who does not comply. Nevertheless, there are difficulties in putting DISHA into practice, particularly in getting informed consent and upholding its rules.¹⁹ The financial burden of putting strong security measures in place might put a strain on clinical facilities' finances. Comprehensive and technologically advanced security measures are required due to the susceptibility of electronically stored data to security breaches. Key components of DISHA's effective proposal include raising awareness of the issue and safeguarding people's rights to privacy and data security.

The Impact of DPDP Act, 2023 in Digital Health Data Protection and Government Surveillance

By limiting the gathering, use, and sharing of personal data and highlighting the significance of only processing personal data for legitimate purposes, the DPDP, 2023 aims to protect individual privacy rights. It will boost patient confidence and trust in addition to enhancing data security and cyber breach control. India is expected to have one of the biggest digital personal data footprints in the world, both at rest and in motion, by 2030 and to have the third-largest economy globally. The importance of the DPDP 2023 Act is demonstrated by our growing influence in the international system. Due to the G20 Presidency and numerous regional and free trade agreements in place, we need to figure out how to solve cross-border free flow of data flows with trust.²⁰

A wealth of sensitive personal data, including genetic information and medical records and treatment histories, are handled by the healthcare industry. It is anticipated that DPDPB 2023

¹⁸ Dwivedi, S.K., 2020. *Personal Data Protection Law in India*, *Legal Developments*. Issue 3, *International Journal of Law Management & Humanities*, 4, p.2136. Available at: <https://www.legal500.com/developments/thought-leadership/personal-data-protection-law-in-india/> (Accessed: 25 November 2023).

¹⁹ *Supra* note 7.

²⁰ Ltd, S.V.P. (2023) *Digital Personal Data Protection act 2023: Impact on Indian healthcare industry*, *LinkedIn*. Available at: <https://www.linkedin.com/pulse/digital-personal-data-protection-act-2023-impact-indian-6j2df> (Accessed: 25 November 2023).

will set strict criteria for the gathering, storing, and handling of this kind of data. To protect patient information, healthcare providers must have strong data encryption, access controls, and audit trails in place. Investments in cutting-edge cyber-security infrastructure will be necessary to comply with these laws, strengthening the healthcare industry's overall resistance to cyber-attacks.

The DPDP, 2023 seeks to provide people more control over their personal information by requiring healthcare organisations to get express consent before gathering, using, or disclosing any personal health data. A major advancement for data privacy in the healthcare sector is the DPDP Act 2023. The Act promotes confidence between patients and healthcare providers by granting people greater control over their personal health information and mandating greater transparency from providers.²¹ The Act does this, among the most significant methods being that it mandates that healthcare practitioners acquire express consent prior to gathering, using, or disclosing any personal health information. Patients now have the freedom to decide who can access and use their data.

For medical consultations, second views, and specialised treatments, healthcare data frequently crosses national borders in today's globally connected society. The bill's provisions pertaining to cross-border data transfers may have an effect on medical tourism and international cooperation. For healthcare organisations, ensuring smooth data flow while upholding the bill's data protection requirements would be essential. Healthcare organisations will need to carefully consider how to maintain the Act's stringent data privacy regulations while still allowing for easy data sharing.

The healthcare industry can face difficulties in adjusting to the strict regulations pertaining to compliance. To prevent data breaches and guarantee compliance, healthcare organisations and providers will need to invest in strong data management systems, encryption technology, and cyber-security measures. Furthermore, getting patients' informed consent can be difficult, especially in urgent medical conditions, and this could delay important healthcare procedures. These expenditures are essential for guaranteeing complete regulatory compliance in addition to preventing data breaches.

Conclusion and Way Forward

Data security and patient privacy are significantly impacted, and these issues require careful consideration. Although artificial intelligence (AI) offers advantages like better data analysis and diagnosis, it also brings with it drawbacks including prejudice, security flaws, data privacy issues, and a lack of transparency. Using a multifaceted approach is required to fully utilise AI in healthcare while protecting patient data²².

²¹ *ibid.*

²² Alanazi, S.D., Alanazi, F.M., Alateek, S.S. and Algufaili, R. (2024) 'The Implications of Artificial Intelligence on Healthcare Data and Information Management: Ensuring Patient Privacy and Data Security', *Saudi Journal of Medicine*, 9(5), pp. 159–162. doi:<https://saudijournals.com/>.

It is crucial that current legal frameworks be continuously improved and adjusted to meet new issues as the field of digital health develops with AI. Although a huge step forward, the Digital Personal Data Protection Act, 2023 could need to be updated on a regular basis to balance with new developments in technology and changing security risks. Stakeholders should work together to identify areas within the current legislations that require explanation, improvement, or alteration. These experts should include legal professionals, healthcare professionals, and technological specialists. The goal of this procedure should be to protect individual health records while maintaining the legal framework's adaptability to the rapidly evolving field of digital health technology.

The successful safeguarding of private health information requires cooperation amongst several parties. Government agencies, healthcare providers, IT firms, legal professionals, and patient advocacy organizations must work together actively on this. Creating a multi-stakeholder task force or advisory board might help with continuing debates, information sharing, and the creation of policies. Constructing inclusive discussions would facilitate a complete comprehension of the issues at hand and the development of all-encompassing, contextually appropriate solutions. This cooperative endeavour need to encompass ethical, medical, and technical viewpoints in addition to legal ones.

Because digital threats are always changing, data security demands a proactive approach to technical innovation. Advanced authentication techniques, block-chain solutions, and state-of-the-art encryption technology may all greatly strengthen the security of personal health data. Furthermore, ongoing research and development in threat detection, incident response skills, and cyber-security measures are crucial elements of a strong ecosystem for digital health. Technology businesses, academic institutions, and government agencies working together can accelerate the creation and use of cutting-edge solutions that safeguard data while preserving the smooth operation of digital health systems.

By enhancing diagnosis, personalising treatment, and streamlining administrative tasks, AI is revolutionising operations and patient care. All of these causes have led to major change in the healthcare industry. When applied to the healthcare sector, artificial intelligence (AI) has the potential to revolutionise data management, improve patient care, and save lives. However, the unique security challenges that the healthcare sector faces—such as human error, medical device vulnerabilities, and regulatory compliance—highlight the importance of AI-driven security solutions. Healthcare data security is crucial since patient data is sensitive and cyber threats are increasing. The legislative framework's transition from the Information Technology Act of 2000 to the more comprehensive Digital Personal Data Protection Act of 2023 has been an essential first step in addressing these concerns. This study has thoroughly evaluated the provisions of the new Act, focussing on its implementation, the rights offered to individuals, the requirements for data handlers, and the enforcement processes. The evolution of laws

protecting private health information in the digital era has been clarified by a comparison with the Act of 2000.

There is a need to strike a balance between the both. Both privacy and technology advocates concur that a careful balance must be struck. Technology must be utilised responsibly and with protections in place if trust is to be established. The inappropriate use of face recognition technology by governments and law enforcement organisations raises legitimate privacy issues, particularly when there is no legislation or policy controlling its application. However, the importance of facial recognition technology for both corporate and law enforcement applications should not be understated. A clear control and guidance framework must be established in order to weigh the advantages of facial recognition against any possible risks.

Furthermore, it's critical to take into account India's advancements in safeguarding private health information globally. Apart from offering a starting point for advancement, a comparison with global data protection laws will yield valuable insights regarding optimal methodologies.

References:

1. The Digital Personal Data Protection Act, 2023
2. Aadhaar (Data Security) Regulations, 2016
3. Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002
4. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011
5. Information Technology Act, 2000 (Act No. 21 of 2000)
6. Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2017
7. The Mental Health Act, 1987” (Act No. 14 of 1987)
8. The Public Financial Institutions (Obligation as To Fidelity and Secrecy) Act, 1983” (Act No. 12 of 1983).
9. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Trans-border Data Flows 2001
10. APEC Privacy Framework, 2015
11. Asia Pacific Economic Corporation Privacy framework 2004
12. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981
13. EU Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data 1995

14. European Convention on Human Rights
15. International Covenant on Civil and Political Rights, 1966
16. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 1980
17. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, (2013)
18. Durga Das Basu, Comparative Constitutional Law (1984)
19. Kothari, C.R “Research Methodology Methods and Techniques” New Age Publications New Delh,2014
20. Pandalai Shruti, “The Social Media Challenge to National Security: Impact and Opportunity” Institute for Defence Studies and Analyses, New Delhi, 2016
21. Ronald E. Leenes, “Data Protection and Privacy: The Internet of Bodies” Bloomsbury Publications, United Kingdom, 2019
22. Sathe,SP , “Right to Know” ,N.M.Tripathi,Bombay,1991
23. Seervai, H. M. “Constitutional Law of India”, 2nd ed. N. M. Tripathi, Bombay,1975
24. Singhvi, L. M: Horizons of Freedom, New Delhi, National Publishing House, 1969.
25. Sinha, B.S: An Introduction to Law of Torts through Indian cases, Eastern Book Company, Lucknow 1999
26. Sinha, Manoj Kumar: Implementation of Basic Human Rights, New Delhi, Manak Publication Pvt. Ltd., 1999.
27. Tripathi, P.K: Spotlight on Constitutional Interpretation, N.M Tripathi Pvt Ltd, Bombay,1972