IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Data Breaches In Healthcare: Examining Cyber Offences And Legal Protection In India

[1]Rishabh Shukla, [2]Dr. Vikas Gupta
[1]Research Scholar, [2]Professor
[1&2] Faculty of Law
[1&2] Jagran Lakecity University, Bhopal

**Abstract:** Healthcare data is one of the most sensitive personal pieces of information that a person creates - it captures not only physical statuses but mental health background, reproductive status, genetic formation, and patterns of behaviour that, when revealed, may lead to discrimination, financial abuse, damaged reputation, and severe abuse of personal dignity. The healthcare industry in India with its fast digitalization and the adoption of electronic health records, telemedicine platforms, insurance portals, and government health schemes like Ayushman Bharat are taking a more appealing form to cybercriminals. There has been a significant increase in the number of data breaches of hospitals, health-tech firms, and state health databases in the country, but the legal framework concerning the protection of health data is fragmented, under-enforced, and, until the recent adoption of the Digital Personal Data Protection Act, 2023, does not include a specific data protection law. In this paper, a thorough review of the Indian healthcare data breach problem is performed using the prism of a cybercrime law and a data protection law. It examines the character and extent of healthcare data breaches, charts out the current legal context such as the Information Technology Act, 2000, the DPDP Act, 2023, and the industry-specific regulations, and critically assesses how these tools are sufficient to prevent breaches and safeguard patients. The paper contends that India is at a crossroad: the IT infrastructure of digital health is being developed on a massive scale and the legal framework of protecting the information that infrastructure produces must be developed equally seriously.

**Index Terms -** healthcare data breach, cyber offences, data protection, DPDP Act 2023, Information Technology Act, patient privacy, India, digital health

## 1. INTRODUCTION

Health information has a certain type of vulnerability that is attached to it. A medical record is not in fact a list of diagnoses and prescriptions, but in itself a kind of an intimate biography, capturing the times of physical adversity, mental illness, reproductive history, genetic susceptibility, and the myriad individual choices that individuals make regarding their bodies and lives. Once that information is revealed, i.e. in the case of a data breach, unauthorized disclosure, or cyber-attack on the institution in which the information is stored, the damage does not just end at inconvenience. It may imply loss of jobs, refusal of insurance, lender or housing prejudice, the rupturing of personal connections and in the worst possible scenario, the targeted exploitation that ensues after delicate individual information is shared with criminal organizations.

The healthcare industry in India is currently undergoing a revolution in digital transformation of some magnitude and pace. In 2021, Ayushman Bharat Digital Mission seeks to establish a single digital health ecosystem that connects patients, providers, payers, and public health authorities using unique health IDs and interoperable electronic health records. Telemedicine platforms have placed millions of patients in the digital health interaction space, and have been catalysed by the COVID-19 pandemic and legal foundation by the Telemedicine Practice Guidelines of 2020. Patients now have huge amounts of data that are stored by health insurance portals, diagnostic chains, pharmacy aggregators and health-tech startups. There are

real gains associated with this digitization; there is enhanced care coordination, less duplication, and enhanced surveillance of the population. It also provides a surface at which cyberattack has never been before.

The magnitude of the threat is not theoretical. In the years 2022 to 2024, India was one of the most targeted countries to be targeted in healthcare cyberattacks in accordance to data collected by cybersecurity firms monitoring threats in the sector. It has been shown that healthcare institutions of all levels of sophistication and resources are susceptible to high-profile incidents- the breach of the All-India Institute of Medical Sciences (AIIMS) Delhi server infrastructure in November 2022, the exposure of data in the CoWIN vaccination portal in 2023, and attacks on numerous chains of private hospitals have shown that even the most sophisticated institutions need to protect their data. The attackers are sponsored by the state to gather strategic information or by ransomware websites to make financial gains or by simple criminals to take advantage of simple security weaknesses.

It is on this background that the legal provisions governing the safeguarding of healthcare data in India has long been, up until not too long ago, conspicuously insufficient. Unauthorized access, data theft, and protection of sensitive personal data are covered in the Information Technology Act, 2000, as amended in 2008, although they were not intended to address the unique features of the healthcare sector. Such a situation created a substantial normative void since no law provides a general data protection statute until the Digital Personal Data Protection Act, 2023 was adopted. Individual sector-based rules set by the Medical Council of India, the Insurance Regulatory and Development Authority, and the Ministry of Health and Family Welfare have tackled aspects of the issue without giving any consistent general set of rules.

In this paper, we will discuss these questions in two mutually complementary frames: the cybercrime law frame, which poses what is criminalized and the means to enforce it; and the data protection law frame, which poses what obligations healthcare institutions have to the data they possess and what remedies patients may seek in case of the violation of their obligations. The paper will follow this procedure by identifying the nature of healthcare data breach in India, discussing the trends of its occurrence, taking a critical look at the legal framework as it stands, evaluating its weaknesses and limitations, and a comparative overview of regulatory practices in other countries with guidelines to achieve a more consistent and efficient system of legal regulation of healthcare data.

## 2. DATA BREACHES IN HEALTHCARE: NATURE, PATTERNS, AND MAGNITUDE.

To know why healthcare institutions have been especially targeted by the cybercriminals, one must first comprehend what makes the health data valuable to those who would misuse it and to those who would protect it. Health data is irreversible whereas financial data can be cancelled and republished in case the latter is compromised. The diagnosis of HIV, prior psychiatric treatment, genetic test outcome, or abortion history of a person may not be altered. The fact that health data cannot be changed implies that its disclosure is an irreversible damage as opposed to a finite and reconcilable issue.

### 2.1 Why Healthcare Data is a favourite Target.

This permanence is reflected in the market value of the health records on criminal data markets. Analyses of the industries have continuously established that full medical history attract much more expensive prices than credit card numbers or social security data on the dark web markets, which is exactly due to the fact that they allow a wider scope of exploitation: insurance fraud, targeted blackmail, identity theft, and profiling of individuals to use them in discriminatory activities. Healthcare institutions provide a favourable target to ransomware operators as they have a sensitive nature, making them highly motivated to pay instead of expose, and as some of the weakest cybersecurity infrastructures as compared to financial institutions in the past.

Another form of structural weakness in healthcare institutions is somewhat sector-specific. Their systems are critical and they cannot be put offline to undertake security maintenance without interfering with patient care. They have huge volumes of interconnected medical equipment - imaging machines, infusion pumps, monitoring machines - which usually operate on older operating systems and cannot be readily upgraded. They hire vast armies of clinical personnel whose initial training is in patient care as opposed to cybersecurity hygiene. And they are custodians of the data on behalf of patients who have not agreed to a specific degree of security risk and only limited capacity of transferring their data to a different party in case they do not like the current level of protection.

**2.2 Healthcare cyber offence typology.**

Computer crimes that result in healthcare data breaches fall under a series of cybercrimes which can be categorized in general based on the type of attack mechanism and attack intent. The most common cyber threat to the hospital systems all over the world, including India, has been ransomware attacks, where malicious software blocks access to the data and the institution must pay to have the data restored. This category was illustrated by the AIIMS Delhi attack of November 2022, which affected the work of the hospital for several weeks and had allegedly breached the data of millions of patients. It was suspected that the attackers in the said attack had ransomed their attack in cryptocurrency and the Computer Emergency Response Team of India described the attack as a specific attack on critical national infrastructure.

The second major category is data exfiltration attacks which are not similar to ransomware since the aim is to steal and sell or weaponize information but not to encrypt information and demand ransom. Phishing debacles on the credentials of healthcare workers, the usage of the weak areas of the hospital management software, and hacked third parties vendor access were all recorded as the means of data exfiltration in the Indian healthcare setting. The CoWIN data leak of 2023, where individual information about those vaccinated, including their health data, tied to their vaccination status, were reported to be accessible in a Telegram bot, demonstrated that health data management systems managed by the government may turn into a breach point.

The third threat category that is frequently overlooked in the context of discussing external cyberattacks is that of insider threats when the participants are employees of the healthcare systems, as well as the contractors or other persons that have a legitimate access to the systems. The healthcare staff who have access to the records of patients can view them due to curiosity, personal reasons, or because of coercion by third parties. The comparative ease of record access in most hospital information management systems together with inconsistent access logging and audit methods makes insider breaches hard to detect and attribute.

| Incident | Year | Nature of Breach | Data Affected | Reported Scale |
|---|---|---|---|---|
| AIIMS Delhi Cyberattack | 2022 | Ransomware / Server Compromise | Patient records, hospital operations data | Approx. 3–4 crore patient records reportedly affected |
| CoWIN Portal Data Exposure | 2023 | Alleged data leak via Telegram bot | Vaccination records, personal identifiers | Reports of widespread personal data exposure; scale disputed |
| Safdarjung Hospital Attack | 2022 | Ransomware | Administrative and patient data | Disrupted hospital operations; scale not officially confirmed |
| HealthTech Startup Breach | 2021 | Unsecured cloud database | Diagnostic test results, personal health data | 68 lakh+ records reportedly exposed |
| Regional Insurance Portal Breach | 2020 | Credential stuffing / unauthorized access | Policyholder health claims data | Several lakh records reportedly compromised |

**Table 1: the number of healthcare data breach incidences in India (2020 2023) selected.**

The above-summarized incidents have some characteristics which are of analytical value. To begin with, they cover the entire range of healthcare data custodians, including government hospitals, government vaccination infrastructure, private chains of hospitals, health-tech startups, and insurance organizations. This weakness is not limited to any type of organization. Second, the amount of data impacted each time an incident occurs is large, in the form of lakhs and crores of records, which is representative of data concentration in centralized health information systems. Third, in a number of instances, the affected institution did not notice the breach immediately, and the news was disclosed to the population by external security researchers or by the media. This failure to detect is actually a failure in monitoring and incident response that is not institution-specific.

## 3. INDIA LEGAL FRAMEWORK OF HEALTHCARE DATA PROTECTION.

India was the first country to have a comprehensive legislation against cybercrime and electronic commerce in the form of the Information Technology Act, 2000 (IT Act). It majorly concentrated in legalizing the electronic transactions and developing a structure to deal with computer related crimes. In 2008, the amendments made under the Act significantly extended the provisions of cybercrime and the establishment of the Section 43A which held a civil liability on corporate entities in the negligent processing of sensitive personal data, and Section 72A, which found guilty of disclosure of personal data in violation of a legitimate contract.

### 3.1 Information Technology Act, 2000 and its Amendments.

Section 43 of the IT Act imposes liability in the unauthorized access to computer systems, downloading or duplicating data without authorization, introducing viruses or malicious code and damaging computer systems. Section 66 prohibits dishonest or fraudulent practices under the provisions of Section 43 that include a jail term of three years and penalties. Section 66C punishes identity theft the untrue use of the electronic signature, the password or some other distinctive feature of identities of another person with up to three-year imprisonment. The section 66D treats personation cheating with the help of computer resources. Section 72 criminalises violation of confidence and privacy by the individuals who may have accessed the electronic records under the auspices of the official responsibilities.

The first regulatory instrument that specifically relates to the security of the personal data in India prior to the DPDP Act is the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 -presented in the frames of the Section 43A. These Rules point out the definition of sensitive personal data or information as passwords, financial data, information on the health and physical condition, sexual orientation, medical records and history, and biometric data. They require that the organizations collecting such data need to have reasonable security practices, ask permission before collecting it, and that the collected data should be used in the mentioned purpose and provided people with an opportunity to gain access to their data. They also need to appoint a grievance officer who will accept complaints of data subjects.

This framework of healthcare data has serious limitations. This is because rules apply to body corporates only, but not to individual practitioners and other healthcare professionals who are not incorporated. Security practices standard on reasonableness is not established by regulation or adjudication and therefore, it was not clear what compliance entails. Civil damages which are payable by the injured person, as envisaged by the regime of penalties in Section 43A, has barely been used in practice at all, partly due to the difficulty in proving and quantifying damage. The IT Act does not provide notification of breaches thus, the breach victims are unlikely to receive information regarding the fact that their health data has been affected**.**

### 3.2 Digital Personal Data Protection Act, 2023.

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the largest amendment to the Indian law on data protection in the years since the amendments of the IT Act in 2008. A system of data principal rights, data fiduciary duties, and a system of enforcement, with a Data Protection Board, is established by the DPDP Act, which was passed after a long legislation process, including a report by the Justice Srikrishna Committee, 2018, a series of reviews by the committee, and failure of the Personal Data Protection Bill, 2019.

The DPDP Act has several provisions that are of particular concern to the healthcare data protection. The Act also applies to digital personal data - data about a person, but processed, stored and accessed using digital methods - and their conditions are subjected to the so-called data fiduciaries who are persons who make decisions about how, and why, personal data must be processed. This definition includes healthcare centers, health technology services, healthcare insurance organizations, and governmental health plans. The individuals involved who are the data principals have a right of access to the information, right to

correct inaccuracies in an information and right to erase information under certain circumstances and the right to appoint a representative to represent them.

The Act requires data fiduciaries to implement its corresponding technical and organizational policies to ensure data protection, disclosure to the Data Protection Board and to the corresponding data principal in the event of a personal data breach, and the use of data as specified within the applicable legal boundaries of the data use in the first place, wherein consent has been obtained or which can be categorized under an established category of lawful use. The consent framework is significant to healthcare: the Act admits that consent given by the employer of the data principal, or by a governmental authority, must be subject to some conditions, and that the Act contains only limited categories of processing that do not require consent to be made - an example of these being medical emergencies and the provision of medical care or any other provision relevant.

This is a DPDP Act enforcement mechanism that contains the Data Protection Board of India which is supposed to receive complaints and conduct an inquiry and impose a fine on the violators of the provisions of the Act. Penalty schedule is large - large penalties, in the hundreds of crores rupees to non-compliance with the provision of adequate security means, it is necessary to inform about the violations of those means, however, the presence of such penalties in the case of violation is determined by whether the Board is institutionally independent, endowed and has a strong commitment to vigorous enforcement or not.

### 3.3 Regulatory Instruments that are Sector-Specific.

Besides the IT act and DPDP act, healthcare information in India is likely to become the victim of various sector-specific regulatory instruments of various scope and depth. The Clinical Establishments (Registration and Regulation) Act, 2010 requires clinical establishments to maintain patient records, and to safeguard the data, does not take a specific reference to cybersecurity or security of digital data. The statements, which the telemedicine platforms must ensure the privacy of the patient data and ensure the safety of data security, are present in the Telemedicine Practice Guidelines, 2020, but are not intertwined with any technical norms and regulatory structures.

The Insurance Regulatory and Development Authority of India (IRDAI) has also issued a guideline on information and cyber security to the insurance companies that have it provide information security management systems and report on cyber incidents to the authority. Indian Electronic Health Records Standards, which were established by the Ministry of Health and Family Welfare, 2016 contains the technical standards of health data exchange interoperability, although it does not address the issue of data security requirements comprehensively. The data governance is provided on a high level in the operational guidelines of the National Digital Health Blueprint and the Ayushman Bharat Digital Mission but not on the security standards, which remain to be determined.

The result of a regulatory environment like this is fragmentation: different kinds of healthcare data holder are governed by different requirements and by different powers and in different ways. The duties of a private hospital associated with the Clinical Establishments Act, the IT Act, the DPDP Act, and the regulations on a state level may be conflicting or overlapping, or they may be irrelevant to each other with regard to the particular security risks. The absence of a single industry-specific data protection standard that would be analogous to the Health Insurance Portability and Accountability Act in the United States of America which is known as the Security Rule, or the Data Security and Protection Toolkit in the United Kingdom, is a sizable gap.

## 4. CRITICAL REVIEW OF THE LEGAL FRAMEWORK.

The constant critique of the system of cybercrime and data protection in India, as it applies to healthcare, is related to enforcement. The IT Act has existed on statute books more than 20 years but the number of prosecution of persons who have accessed health information without authorization and those that have dealt carelessly with sensitive personal information is infrequent. The Adjudicating Officers designated in accordance with Section 46 of the IT Act to adjudicate civil claims, such as claims in accordance with Section 43A of negligent data handling claims, have a poor record of health data disposals. The national computer emergency response team, CERT-In, deems the breach reports and provides advice, yet it does not have the mandate to issue penalties or enforce remedies on specific cases.

### 4.1 The Problem of Enforcement

The constant critique of the system of cybercrime and data protection in India, as it applies to healthcare, is related to enforcement. The IT Act has existed on statute books more than 20 years but the number of prosecution of persons who have accessed health information without authorization and those that have dealt carelessly with sensitive personal information is infrequent. The Adjudicating Officers designated in accordance with Section 46 of the IT Act to adjudicate civil claims, such as claims in accordance with Section 43A of negligent data handling claims, have a poor record of health data disposals. The national

computer emergency response team, CERT-In, deems the breach reports and provides advice, yet it does not have the mandate to issue penalties or enforce remedies on specific cases.

There was still no mechanism of enforcement, the Data Protection Board, in operation as at the time of writing this article, and the rules under the DPDP Act were yet to be notified. Further questions of institutional design that the Board still needs to address will be whether the Board is adequately staffed and adequately funded, whether the Board has a record of real enforcement and is not a complaint-process agency with no deterrent effect. Practice across most data protection regulators in other jurisdictions indicates that institutional culture and regulatory philosophy are at least as important as the formal powers available under statute.

**4.2 Gaps in the DPDP Act in the coverage of health data.**

Although the DPDP Act is a major step forward, there are a number of areas relating to its application to healthcare that should be noted. To begin with, what the European Union has offered under the General Data Protection Regulation as sensitive or special category personal data, the Act does not provide, and the processing of such data involves increased protection, which is more demanding on the consent of people and imposes additional limitations on the processing of health data than on the processing of ordinary personal data. What is missing is the differentiation so that health information, even though it is of a sensitive nature and the harm that arises after its disclosure is severe, is not exempt of the general duties imposed in less delicate areas of personal information.

Second, the consent model in the Act, though well-conceived, can cause some practical challenges in healthcare. Achieving a specific, informed and freely given consent to each type of data processing in an acute care setting, where a patient might be in distress, where deciding to treat a patient may require rapid decision-making and where data is regularly and routinely shared among multiple providers is operationally complicated. The legitimate uses exceptions, which allow the processing without consent in medical emergencies and in providing healthcare, are valuable provisions but their scope in the healthcare context, which will need some regulation, will have to go through adjudication in the end.

Third, the application of the Act to government bodies, which maintain some of the biggest repositories of health data in India, such as the Ayushman Bharat Digital Mission databases and the CoWIN vaccination record, contains certain provisions that restrict their responsibilities as compared to those of data fiduciaries in the private sector. Data fiduciaries of a government are not subject to all the rights of erasure and correction, and the mechanism of enforcement is different than the mechanism of enforcement of it on a private entity. Since the government health data base has been one of the most conspicuous environments where data has been exposed over the past few years, the suitability of this differentiated treatment has been questioned.

**4.3 The Limitations of the Cybercrime Law in the health care setting.**

The IT Act provisions of cybercrime were created as multi-purpose tools and demonstrate their obsolete in the healthcare setting. The definitional framework, which was centered around the concept of computer systems, computer networks, and electronic records, fails to take into consideration the specific aspects of the healthcare sector, namely, the presence of the Internet of Things devices that currently pervade clinical settings, the sensitivity of health information in comparison with other types of personal information, or the aspect of public interest to the security of healthcare infrastructure that underlies the classification of attacks on hospitals as an attack on critical national infrastructure.

The IT Act penalty framework does not distinguish between cyberattacks on hospitals that have the potential to damage life-critical services and reveal some of the most personal information of the patients and an attack targeting a commercial system of minor social significance. Sentencing guidelines in Sections 43 and 66, which govern unauthorized access and data theft, allow up to three years in prison, which critics have claimed is not severe enough to discourage highly organized and professional cyber criminal activities of the nature that result in major ransomware attacks. The Bharatiya Nyaya Sanhita, 2023 effective in July 2024 to replace the Indian Penal Code does not directly cover crimes against healthcare data, meaning the IT Act remains the most commonly used criminal law tool in this field.

**5. COMPARATIVE PERSPECTIVES**

The principles of GDPR informed the DPDP Act of India but deviates in a number of key ways, such as lack of special category framework of health data and some restrictions on the rights of data principal with respect to government entities. These departures are either necessary to the situation in India, or they are loopholes that weaken the securities of the health data framework and it is a question that practitioners and the Data Protection Board will have to answer in the same act implementation.

### 5.1 HIPAA Model: The Sector-Specific regulation.

The most significant model of healthcare data regulation in the world is the United States Health Insurance Portability and Accountability Act of 1996 (HIPAA) including its Privacy Rule and Security Rule regulations, which impose the most influential model of sector-specific healthcare data regulation worldwide. HIPAA is binding on both covered entities (healthcare providers, health plans and healthcare clearinghouses) as well as business associates that process the protected health information on their behalf. Its Security Rule mandates covered entities to adopt administrative, physical, and technical controls to safeguard electronic health information with its requirements being based on the risk profile of health information. The Breach Notification Rule obliges covered entities to conduct notification to the affected individuals, the Department of Health and Human Services and in case of major breaches to the media within the designated time frames.

HIPAA model has not been without critics: some have described it as compliance-oriented as opposed to security-oriented, producing lots of administrative burden, yet without necessarily improving security outcomes. Its civil and criminal penalty framework has, nevertheless, delivered a history of substantial execution - including multi-million-dollar settlements and criminal indictment - that have helped to instil a culture of data security adherence into the US healthcare industry. The technical standards and enforcement mechanisms specific to the healthcare risk profile, enabled by the sector-specific nature of the framework, is the element most directly applicable to the situation in India.

### 5.2 Treatment of Health Data by the GDPR.

Since 2018, the General Data Protection Regulation (GDPR) of the European Union considers health data as one of the special categories of personal data and provides it with a much higher protection level. Health data processing is in principle forbidden except where the subject of the data has provided express consent or where at least one of a specified group of exceptions applies exception that covers processing required to provide medical diagnosis, health/social care or reasons of public interest in the field of public health. Data Protection Impact Assessment requires healthcare organizations to evaluate the new data processing activities involving health data before they are implemented. The breach notification provisions of the GDPR provide that seventy-two hours of learning about a breach and providing notice to the supervisory authority and forty-eight hours of learning about a breach and informing affected individuals should follow without undue delay.

## 6. DEVELOPING A COHERENT FRAMEWORK: REFORM PROPOSALS.

The discussion above leads to a list of priorities to enhance the legal framework regarding the healthcare data protection in India. These suggestions are aimed at the content of the law and institutional structures of its enforcement.

The most significant structural change is the introduction of a specific Healthcare Data Protection Rule under the DPDP Act - relying on the authority of the Act to communicate sector-specific rules. This rule must come up with some set of standards of security of the holders of healthcare data based on the sensitivity of health data and the particular vulnerabilities of healthcare IT systems. It must impose routine security audits, vulnerability testing on healthcare organizations, enforce access controls and audit logs to specified minimum standards, and prepare and test incident response plans. The standards must be differentiated depending on the size and capacity of an organization, and small providers should have proportional responsibilities, but big hospitals and health-technology platforms must have strong security baseline.

The healthcare sector rule as an uncompromising condition needs to be operationalized by making mandatory breach notification to both the Data Protection Board and the affected patients within a specified period with specific content requirements. The fact that the current mandatory notification regime lacks functionality implies that patients who have had their health data breached regularly do not have a way of learning about the incident or take a precautionary measure. Accountability incentives can also be created by notification requirements, which are effectively enforced: the institutions aware of the necessity to notify the regulators and patients of a breach will have greater incentives to avoid breaches in the first place.

The mandate of CERT-In must be clearly expanded to include healthcare critical infrastructure with specific sector-specific capabilities of responding to cyber incidents in hospitals and health data platforms. The AIIMS Delhi attack proved that a cyberattack on one of the largest hospitals is not just the data protection issue, but it is the problem of patient safety and emergency which affects the work of clinical services and may directly threaten the life of patients. The institutional reaction to these incidents involves not only IT security skills but also knowledge of the clinical practice and skills in association with the

healthcare administrators and regulators. This would be filled by a special healthcare cyber incident response capability of CERT-In or other related bodies.

Medical healthcare cybersecurity capacity building - through industry-specific guidelines, hospital IT employee education and training, and grants to smaller providers to replace their security infrastructure are needed should regulatory needs be achieved in reality and not on paper. The security gains as will come with the regulatory framework, however well crafted will only be realized when the regulated subjects possess the knowledge and resources to apply them. It is this that the Ministry of Health and Family Welfare in liaison with NASSCOM and the professional bodies concerned ought to create a sustainable healthcare cybersecurity capacity-building programme.

Lastly, the patients must be able to sue and have their case effectively remedied in case their health information is compromised, which involves actively building the Data Protection Board complaint system and, where suitable, civil courts. The financial penalty statutes of the DPDP Act do produce deterrence, but the penalties are focused on the State and not on individuals victims. The individual harm aspect would be met by a compensation scheme of data subjects who have sustained real injuries through breaches of healthcare data based on the monetary fines raised, which would enhance the deterrence of breach.

## References


### Statutes, Rules, and Regulations

1. The Information Technology Act, 2000 (Act No. 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009).
2. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
3. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
4. The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.
5. The Clinical Establishments (Registration and Regulation) Act, 2010 (Act No. 23 of 2010).
6. The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023).
7. Ministry of Health and Family Welfare, Telemedicine Practice Guidelines, 2020 (Government of India, 25 March 2020).
8. Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security for Insurers, 2017 (IRDAI Circular No. IRDA/IT/GDL/MISC/168/10/2017).
9. Ministry of Health and Family Welfare, Electronic Health Record Standards for India, 2016 (Government of India, 2016).

### International Instruments and Comparative Legislation

1. Health Insurance Portability and Accountability Act of 1996, Pub L No. 104-191, 110 Stat 1936 (United States).
2. HIPAA Privacy Rule, 45 CFR Parts 160 and 164 (United States Department of Health and Human Services).
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation) [2016] OJ L 119/1.
4. Health and Social Care (Safety and Quality) Act 2015 (UK).

### Reports and Official Publications

1. Ministry of Electronics and Information Technology, Report of the Committee of Experts on a Data Protection Framework for India (Justice B.N. Srikrishna Committee Report, Government of India, July 2018).
2. CERT-In, Annual Report 2022-23 (Ministry of Electronics and Information Technology, Government of India, 2023).
3. National Health Authority, Ayushman Bharat Digital Mission: Annual Report 2022-23 (Ministry of Health and Family Welfare, Government of India, 2023).
4. Check Point Research, 2023 Mid-Year Cyber Attack Trends: Healthcare Among Most Targeted Sectors (Check Point Software Technologies, 2023).
5. IBM Security, Cost of a Data Breach Report 2023 (IBM Corporation, 2023).
6. NASSCOM, Cybersecurity in Indian Healthcare: Emerging Threats and Responses (NASSCOM, 2022).

**Books and Journal Articles**

1. Bhatia, Gautam, The Transformative Constitution: A Radical Biography in Nine Acts (HarperCollins India, 2019).
2. Chander, Anupam, 'Is Data Localization a Solution for Schrems II?' (2020) 23(1) Journal of International Economic Law 91.
3. Dinev, Tamara and Hart, Paul, 'An Extended Privacy Calculus Model for E-Commerce Transactions' (2006) 17(1) Information Systems Research 61.
4. Gluck, Jason, 'Healthcare Data Breaches: A Systemic Failure of Law, Technology, and Policy' (2018) 35(2) Computer Law and Security Review 180.
5. Khanna, Tarunabh, 'Privacy as a Human Right' (2018) 84 Brook L Rev 1227.
6. Purtova, Nadezhda, 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Law, Innovation and Technology 40.
7. Ratan, Shubham, 'Cybersecurity Vulnerabilities in India's Digital Health Infrastructure: A Legal Assessment' (2022) 7(2) Indian Journal of Law and Technology 45.
8. Schwartz, Paul M. and Solove, Daniel J., 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86(6) New York University Law Review 1814.
9. Sharma, Aditya, 'Data Protection in the Healthcare Sector: Gaps in India's Emerging Legal Framework' (2023) 15(1) Journal of Indian Law and Society 112.
10. Solove, Daniel J. and Hartzog, Woodrow, 'The FTC and the New Common Law of Privacy' (2014) 114(3) Columbia Law Review 583.
11. Swire, Peter and Ahmad, Kenesa, 'Encryption and Globalization' (2012) 23(2) Columbia Science and Technology Law Review 416.