International Research Journal of Multidisciplinary Scope (IRJMS), 2024; 5(3):1043-1057 IRJMS

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2024.v05i03.0883

Protecting Personal Health Information in Digital Age: Exploring Indian Legal Perspective

Niharika Raizada*, Mamata Biswal

Gujarat National Law University, Gandhinagar, Gujarat, India. *Corresponding Author's Email: niharika95raizada@gmail.com

Abstract

The adoption of Electronic Health Records (EHRs) in India has been rapid and the significance of protecting privacy of personal health information has proportionally increased as well. The research emanates from scenario of rapidly rising frequency of cyber-threats to personal health information and lower efficiency of the legal framework in handling such threats. The latest development made towards protection of general digital information Digital Personal Data Protection Act, 2023 ensures protection of digital personal data and incorporates important provisions which were not available in the former legislations and regulatory frameworks. However, the aforementioned Act still lacks several significant provisions in comparison to other legislations governing personal health information in other countries. The research identifies several lacunas existing in the Indian legal landscape which can consequently lay an adverse impact on the privacy of personal health information. Furthermore, it also analyzes the legal framework and further conducts a comparative review of the legislations in European Union and United States. The comparative assessment highlights absence of several provisions in Indian legal framework and consequently affecting the data privacy of health information. The analysis following the comparative assessment lays down broad spectrum of provisions which can be incorporated in the Indian legislative structure.

Keywords: Cyber-Security, Cyber-Threats, Data Privacy, Electronic Health Records (EHR), Healthcare, Health Data.

Introduction

Electronic health records are, in simpler language, are electronic versions of the medical records stored and organized by the healthcare service providers like hospitals, clinics and the internet of medical things (IoMT). They consist of patient history that can be referred to or interoperate between hospitals (1). These include essential administrative as well as the clinical data that are basically the care and services given to an individual by a health provider. These are inclusive of details such as demographics, progress reports, problems, medications, important signs, MRI and CTC scans, medical history, immunization reports, laboratory data, radiology reports, etc. (2). The electronic health records have reduced a huge workload of maintaining accounts of medical information of patient but it also increased the susceptibility of illegally access to such medical information (3).

A report published by Quick Heal in 2021 (4) highlighted that India has suffered most cyber-attacks along with 24 other countries. Of these attacks, most of them were targeted at hospitals, government bodies and defense. The cyber-attacks shot up during the period COVID-19 with several number of cyber-incidents covering areas like spyware attacks (5), Distributed Denial of Service Attacks, ransomware (6), digital fraud (7), panic, disinformation, etc. The cyber-incidents levered an approximate cost around in millions and exposing the critical data to the illegal assessors. The data of patients and users of various medical services were accessed without consent and sold to various third parties. However, primary question here is why would they target the medical data which happens to be a sensitive data and what would hackers do with our data? The answer in brief is the medical infrastructure has an issue of weak cybersecurity which attract the hackers and make it easier for them to commit data theft. Also, the stolen data is either sold on the deep dark online market which can enable the buyer on the market commit felony cases like tax evasion, identity theft, etc. The importance and the utter necessity of cybersecurity comes into play when the very fact is highlighted that the patient's data stored and compiled as Electronic Health Records are often stolen and utilized in identity thefts or more

(Received 2nd April 2024; Accepted 19th July 2024; Published 30th July 2024)

serious offences like tax evasion (8). There are thousands of malware attacks infecting the databases of the hospitals, laboratories, devices, etc. and gaining the access to our personal data stored, illegally (9).

Healthcare organizations face several cybersecurity issues every year. In U.S. approximately 88% of healthcare organizations have faced some form of cyber-attack which are usually in form of ransomware attacks, cloud compromise, phishing emails and supply chain attacks (10). Such cyber-incidents have caused healthcare organizations to suffer losses for more than 100 million USD and have also affected the patients or the end-users availing the services. It is also important to note that these incidents are not limited to within international borders, but have also occurred in Indian Territory and have been adversely affecting the Indian healthcare infrastructure and subsequently deteriorating the data privacy of individuals. The event which brought the concern relating to privacy of personal health information into light was ransomware attack on All India Institute of Medical Sciences, New Delhi in 2022. The perpetrators held hostage of one terabyte of digital information of patients and temporarily halted the operations of the hospital. Another event which should be brought in light against this backdrop is data breach incident on Indian Council of Medical Research and CoWIN patient directory in 2023. These incidents although seem harmless but have dire effects on the victims whose data have been stolen or accessed illegally. Such stolen data are susceptible of being misused in several ways; for instance in identity theft or conducting fraud based on financial information of the victims obtained through such breach.

The legal machinery involved in protection of personal health information in India involves several enforceable legislations as well as regulatory frameworks and guidelines. The first legislation focused at information security is Information Technology Act, 2000 and its corresponding rules. Since then, National Cyber Security Guidelines, 2013 was formed as a guiding document for different entities for adoption of best practices and later, Digital Personal Data Protection Act, 2023 (Several bills precede the current bill in motion in the Parliament. Bills like Personal Data Protection Bill, 2018; Digital Information in Healthcare Security Act, 2018 and Data Protection Bill, 2019 were prior attempt at making flawless framework for governing of digital health data specifically) was enacted specifically for the purpose of protection of digital privacy. There is no set legal framework to govern personal health information. The lack of concrete law only makes the electronic health records vulnerable to several issues relating to cyber security like data extortion, identity theft, malware attacks, selling of sensitive records in black market, etc. The article is based on thorough review of literature and includes analysis of legislative framework in India governing the privacy of health information. The analysis of the literature retrieved from secondary sources is conducted with the aim to identify different forms of cyber-threats to which patient information are susceptible and also brings into its ambit, the annual reports published by private organization to underscore the need to address the issue concerning the rising frequency of cyber-threats to healthcare infrastructure. Consequently, the basis of selection of such secondary sources have been to the extent of such research articles, review papers and comments where the concerns relating to different forms of cyber-incidents and their rising frequency have been addressed. The primary objective of the study is to analyze the present legal framework in force to protect digital health information in India and identify possible gaps which needs to be addressed and subsequently will aid in reducing the risk of violation of patient privacy and security of health information.

Methodology

The research adopts normative method and further implements doctrinal method for the purpose of analyzing legal provisions. The research primarily focuses on norms, legal concepts and principles. It also employs primary as well as secondary sources for literature. The research furthermore takes into consideration the statutory approach and examines laws and regulations related to current legal issues for the purpose of formulation of a legal ratio. Primary sources include statutory materials, official records and guidelines. Besides this, as secondary sources, wide-ranging literature from journals, books and commentaries were referred to.

Results

The peculiar sensitive nature of digital health information is known internationally in order to ensure that data is protected specifically (11). It is essential to prevent privacy from being infringed in order to utilize for better prospects like patient care, progressive public health and research purposes (12). The Indian legal and regulatory frameworks lack certain provisions rendering current framework as inadequate. It is important to note that these legal instruments were not brought in force for the purpose to promote the progressive research and improve public health rather they are established for obsolete and redundant technologies (13).

Primary Legislations and Policies

Constitution of India, 1950: In India definition of privacy has been framed by both Indian Judiciary and the Legislature. After a review of literature discussing different aspects of privacy, it can be laid down that in Indian Scenario privacy can be subjectively categorized into four aspects (14), a. privacy and press freedom b. privacy and surveillance c. privacy and decisional autonomy and d. informational privacy. However, we will be discussing all of them briefly but our primary focus is laid upon information privacy. Freedom of expression has been enshrined as constitutional as well as fundamental right in India under Article 19 of the *grundnorm*. Right to privacy has also been given a status of a fundamental right under Article 21 (15).

The conflict situation was laid rest by the Supreme Court in the case of R. Rajagopala v. State of Tamil Nadu (16). The Hon'ble Supreme Court highlighted that only private and confidential information related to national security shall remain out of the ambit of right to information (17). Second aspect of privacy, surveillance has been lately the most discussed part of privacy. With recent upsurge in technology and public policies, surveillance especially by the state has been in focus because it leads to gross violation of digital and manual privacy. In India, privacy has been claimed in two aspects, in property and in communications, however in earlier times, the notion of privacy did not hold a significant status in the eyes of law. The concept of privacy was denied the status of fundamental right in M.P. Sharma v. Satish Chandra (18) and Kharak Singh v. State of Punjab (19, 20). In Kharak Singh case (21), surveillance related constitutional claim of privacy was challenged and the concept of privacy was acknowledged. In Kharak Singh (22), the court was not concerned with the concept of privacy for a while; however, in the next case R.M. Malkani v. State of Maharashtra (23) the Apex Court held that attaching a recording device to a telephone line did not violate section 25 of the Telegraph Act. Even though the judicial pronouncement laid down was related to admissibility of evidence but the Hon'ble Supreme Court denied Article 21 based privacy claim. Subsequently, in the case of Gobind v. State of Madhya Pradesh (24), like in Kharak Singh (25), involved police visits at the personal property of a history-sheeter. The court in this case inclined towards recognizing and determining the right to privacy as constitutional and a fundamental right under Article 21 but instead declared privacy, a right subject to 'compelling state interest' (26). The right to privacy was finally given the status of fundamental right in K.S. Puttuswamy v. Union of India (27) where it overruled both MP Sharma (28) and Kharak Singh (29). The Puttuswamy case (30) put forth a three-tier test to check whether a legislation infringes the right to privacy. The first tier is concerned with legality, the second concerned with requirement, i.e. legitimate objective to enact that particular law and lastly, the third tier of proportionality where the burden is on the state to highlight the legitimate aim supposed to be achieved. In addition to this, the Puttuswamy judgment also highlighted that "privacy is not surrendered just because an individual is in public sphere". The court asserted that privacy is an inherent part of living a life with dignity.

Regardless of this judgment, privacy does not have a status of absolute right. In 2018, the Apex Court laid down in Puttuswamy (II) that AADHAR Act was not unconstitutional and invalid since the intrusion of privacy is proportional to the objective of the legislation. The judgment laid down in 2018 was formed based on 2017 decision. In Puttuswamy (II), Justice Sikri, laid down a four-pronged test to confirm proportionality of the legislation. The first prong is ensuring that a provision restricting a right must be legitimate; secondly, such provision must be appropriate for furthering the concerned goal; thirdly, there must be another alternate remedy available and lastly, the provision should not disproportionately affect owner of the right. Upon analysis of constitutional

validity of AADHAR Act on the above four parameters, the majority inclined towards upholding the constitutional validity of the Act and barred some of its provisions. The court held that AADHAR being a unique and biometric identity system is effective and meets with the conditions of necessity and hence constitutional.

The issue regarding privacy in healthcare was brought up in Mr. Xv. Hospital Z where Mr. X was diagnosed with HIV+ when donated blood. It was alleged that unauthorized disclosure of his positive result of his ailment by the hospital led to Mr. X's marriage and seeking legal course. The court held that doctors are obliged with the irrefutable duty to maintain confidentiality of their patients. However, the court asserted, "public interest would override the duty of confidentiality, specifically where there is an immediate or future health risk to others". In this situation, there was an inherent risk to the health of the woman Mr. X was going to marry.

It is important to note that although Right to Privacy has been given the status of a fundamental right under Article 21, but such status is not absolute, rather it is a qualified right. It is subject to certain restrictions and such restrictions vary case to case.

Information Technology Act, 2000: Information Technology Act, 2000 is a comprehensive legislation focused on governance of several different electronic transactions and interchange electronic data. The Act came into force on June 9, 2000 and specified in its Preamble "An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as ―electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies (Information Technology Act, 2000)" IT Act lays down provisions for various offences (31) under Chapter IX. The Act does not explicitly address data breaches or cyber-attacks. Nonetheless, it stipulates that corporate entities must provide compensation if they fail to protect sensitive data from theft or unauthorized access (32). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, is a pertinent regulation aimed at the explicit protection of sensitive personal data and information, and these Rules are intended to be read in conjunction with Section 43A (33).

Rule 3 of the IT Rules, 2011 (34) defines Sensitive Personal Data and information comprising of information relating to:

1. "password;
2. financial information such as Bank account or credit card or debit card or
3. other payment instrument details ;
4. physical, physiological and mental health condition;
5. sexual orientation;
6. medical records and history;
7. Biometric information;
8. any detail relating to the above clauses as provided to body corporate for providing service; and
9. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise".

Analysis: The Rules although provide for umbrella provisions for protection of sensitive data and information but it does not provide for specific provisions and classification of health and medical data and as to what kinds of data constitute as health data. Furthermore, the Rules have major application over body corporate only and not on other organizations or individuals. Consequently, there won't be any imposition of compensation on individuals or other organizations which are not within the ambit of 'body corporate' (35).

Electronic Health Records Standards, 2016: The Electronic Health Records Standards, 2016 (36) delineates comprehensive standards specifically applicable to healthcare institutions and any entities involved in the creation of medical histories and records. These standards address existing gaps concerning terminologies, protection, and prevention of unauthorized access, particularly in relation to health data. They establish international benchmarks for the protection of sensitive data, as well as for the maintenance, sharing, and enhancement of interoperability of electronic health records. Additionally, the Standards set forth guidelines pertaining to network connectivity, interoperability, and data ownership. Most notably, they provide detailed definitions and

distinctions. 'Electronic Health Record (EHR)', 'Electronic Medical Records' (EMR), Electronic Personal Health Information' and 'Personal Health Record' (EPR).

a. Electronic Health Record: EHR has been defined as "one or more repositories of information in computer processable form, relevant to the wellness, health and healthcare of an individual, capable of being stored and communicated securely and of being accessible by multiple authorised users, represented according to a standardised or commonly agreed logical information model" (37).
b. Electronic Medical Record: EMR has been defined as a varied form of EHR ", restricted in scope to the medical domain or at least very much medically focused" (38).
c. Electronic Personal Health Information: E-PHI has been defined as any protected health information which has been 'created, stored, transmitted, or received electronically' (39). The data thus generated, recorded, delivered, transferred or received through any electronic medium is covered under this term.
d. Personal Health Record: A PHR has been defined as documentation of any form of patient information including medical history, vaccinations or even medicines prescribed and purchased (40).

Analysis: The EHR Standards, 2016 is although an inclusive document but lacks enforceable character due to unavailability of such provision. Subsequently, due to lack of enforceability, the application and the norms so provided within the same, act as mere recommendations or guidelines for health service providers and hence there is no imposition of penalty or fine on lack of implementation of such standards by the service providers.

The Digital Personal Data Protection Act, 2023 (DPDPA, 2023): DPDPA, 2023 is a comprehensive legislation for the governance of the personal digital data. It has been provided in the Act that "The purpose of this Act is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto" (41). The Digital Personal Data Protection Act (DPDPA), 2023 ensures that personal data is processed only after consent and for legitimate uses (42). The consent of an individual is supposed to be "free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose (43)". The consent sought should be followed by conveying all the relevant information describing the purpose of processing such data (44). Section 7 stipulates that data so processed is "for legitimate purposes" along with the condition that Data Principal has willingly provided the personal data and "has not indicated to the Data Fiduciary that she does not consent to its use". Besides this, data fiduciary can also process medical data of data principal in two other scenarios:

a. "for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual (45).
b. for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health" (46).

Section 2 (s) of DPDPA provides additional provision provides for "Significant Data Fiduciary" (30). A significant data fiduciary is "Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10" (47). A significant data fiduciary is appointed by Central Government on the basis of different factors including:

a. "the volume and sensitivity of personal data processed;
b. risk to the rights of Data Principal;
c. potential impact on the sovereignty and integrity of India;
d. risk to electoral democracy;
e. security of the State; and
f. public order" (48, 49).

Analysis: The relevant provisions highlighted do not address the issues relating to privacy, security and confidentiality of health information specifically and most importantly, it does not define sensitive personal data and differentiate between sensitive and non-sensitive personal data. Consequently, there are no provisions for regulation of the same. The sensitive characteristics of EHRs require a comprehensive

legislation which not only identifies and defines personal health information but also anticipates the dynamic and ever-evolving kinds of risk and threats, sensitive information is prone to and subsequently formulate the governing legislation.

Regulatory Framework

National Cyber-Security Policy, 2013: National Cybersecurity Policy, 2013 (NCP) is a comprehensive document which enable different businesses, citizens and government bodies to establish a resilient and secure cyber ecosystem. The NCP, 2013 aims to achieve following objectives:

1. To establish a resilient cyber-ecosystem and develop trust and confidence in IT systems and transactions which take place in a cyberspace.
2. To formulate framework to design security policies and promote and enable global security compliant standards and practices.
3. To establish a stringent regulatory framework to ensure a protected cyber ecosystem.
4. Establish and develop machinery to obtain significant information with reference to risks to ICT infrastructure, creation of solutions for response, risk management and assessment procedures by way of "predictive, preventive, protective, response and recovery actions."
5. Enhance protection of critical infrastructure and establish a 24x7 National Critical Information Infrastructure Protection Centre and mandate security and privacy practices.
6. Introduce and develop technologies for purposes of National Security.
7. Improve transparency and integrity of different technologically connected products and services by developing systems for testing and validation of security.
8. To upscale the number of professionals in cybersecurity.
9. Ensuring fiscal benefits for organizations adopting security standards and practices.
10. Reducing economic losses due to cybercrimes and data theft by protecting information.
11. To enact an efficient prosecution and investigation of cybercrimes through legislative intervention.
12. Enable cybersecurity culture and privacy enabled responsible behavior.
13. To develop public-private partnerships.
14. To promote and develop global cooperation towards furthering the cause of security in cyberspace.
15. Establishment of such mechanisms which provide for early warnings, risk and response management.
16. To formulate a framework for assessment for conformance and compliance certification to best cyber practices and policies.
17. Reduction of supply chain risks in cyber infrastructure.

Analysis: It is relevant here to know that National Cybersecurity Policy, 2013 is although a comprehensive document but does not introduce provisions to mandate organizations and corporations to establish an internal policy in compliance with the NCP, 2013. Besides this, the policy is more like a guiding stick in the dark and developing room of technology, which will turn obsolete in coming time. The policy does not, moreover, introduce any rights, obligations of data owner or consent. Even though it's a holistic framework having preventive characteristics but it does not cover enough area to protect sensitive data.

Comparative Assessment of the Indian Legislation in Relation to International Counterparts: Upon analysis of Indian legal and regulatory framework, it can be stated that Indian legal framework suffer from several shortcomings. An assessment of legal framework implemented in International counterparts, primarily United States and European Union will provide an overview of provisions, which can also be incorporated in Indian legal regime. The comparative assessment of Health Insurance Portability and Accountability Act enforced in U.S. and General Data Protection Regulation applicable on member states of European Union with DPDPA and IT Act currently in force in India will provide a comprehensive view of provisions primarily dedicated to protection of personal health information. The table (Table 1) below compares and assesses the provisions on their scope, applicability along with respective clauses concerned with rights and duties of data owners and responsibilities of data fiduciaries. The assessment is followed by detailed analysis (Section 5) based on the table below.

Table 1: Comparative Analysis (Source: the Information Technology Act, 2000 (IT Act) and Digital Personal Data Protection Act, 2023 (DPDPA); Health Insurance Portability and Accountability Act, 1996; General Data Protection Regulation)

	Information Technology Act, 2000 & Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (India)	**Digital Personal Data Protection Act, 2023 (India)**	**General Data Protection Regulation, 2018 (European Union)**	**Health Insurance Portability and Accountability Act, 1996 (United States)**
Applicability	Section 43A, Explanation Covers Body Corporate and not government organization.	Section 2 (1)(*i*) Data Fiduciary Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data	Section 2 Definitions This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	Section 164.104 Applicability • A health plan. • A health care clearinghouse. • A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. • Where provided, the standards, requirements, and implementation specifications adopted under this part apply to a business associate.
Health Data/ Personal health information/ Medical data/ Sensitive Data	Section 2 (1) (o) "Data" Representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer	Section 2(1) (t) "Personal data" Any data about an individual who is identifiable by or in relation to such data	Article 4 "Personal Data" Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an	Section 160.102 Definitions "Health Information" Health information means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university,

system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer		identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
Clause 3, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011		Article 2 (15) "Data Concerning Health"	"Protected health information"
"Sensitive Data"		Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status	Protected health information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.
Rule 2 (i), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011			"Electronic protected health information"
"Personal information"			Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section.
Any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.			

Consent	No Clause	Section 6 Consent The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.	Article 7 Conditions for Consent If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.	No specific provision but deals with it under other Sections.
Transfer Of Information	On consent of information provider (Section 7)	No explicit provision	No specific provision but deals with it under other Sections.	No specific provision but deals with it under other Sections.
Disclosure Of Information	On consent of information provider (Section 6)	No explicit provision	No specific provision but deals with it under other Sections.	Section 164.502 Uses and disclosures of protected health information: General rules. Section 164.504 Uses and disclosures: Organizational requirements. Section 164.506 Uses and disclosures to carry out treatment, payment, or health care operations. Section 164.508 Uses and disclosures for which an authorization is required. Section 164.510 Uses and disclosures requiring an opportunity for the

				individual to agree or to object Section 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required
Collection Of Information	On consent of information provider (Section 5)	No specific provision but deals with it under other Sections.	No specific provision but deals with it under other Sections.	No specific provision but deals with it under other Sections.
Rights Of Data Principal	No specific provision but deals with it under other sections implicitly.	Article 11 Right to access information about personal data. Article 12 Right to correction and erasure of personal data. Article 13 Right of grievance redressal. Article 14 Right to nominate	Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject Article 13 Information to be provided where personal data are collected from the data subject Article 14 Information to be provided where personal data have not been obtained from the data subject Article 15 Right of access by the data subject Article 16 Right to rectification Article 17 Right to erasure ('right to be forgotten') Article 18 Right to restriction of processing Article 19 Notification obligation regarding	No specific provision Section 2, Definitions Business associate means, with respect to a covered entity- • A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information. • A person that offers a personal health record to one or more individuals on behalf of a covered entity. • A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate. Covered entity means: • A health plan.

			rectification or erasure of personal data or restriction of processing Article 21 Right to object	• A health care clearinghouse. • A health care provider who transmits any health information in electronic form.
Risk Assessment And Management	Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 Section 8 The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements"	No Clause	Article 32 Security of Processing Recital 75 Risks to the Rights and Freedoms of Natural Persons Recital 76 Risk Assessment Recital 77 Risk Assessment Guidelines Recital 78 Appropriate Technical and Organizational Measures Recital 79 Allocation of the Responsibilities Recital 83 Security of Processing	Sec. 164. 308 Administrative Safeguards • Risk Analysis (Required) • Risk Management (Required) • Sanction Policy (Required) • Information system activity review (Required)
Duties Of Data Fiduciary	No specific provision but deals with it under other Sections.	Section 8 General obligations of Data Fiduciary Section 10. Additional obligations of Significant Data Fiduciary	Article 32 The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Article 24 Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons Article 25	No specific provision but deals with it under other Sections.

			The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.	
Data Retention Period	No clause	No clause	Organizations *must make sure that information relating to health is not kept on their files for longer than* necessary.	6 years
Data Breach Notification	No specific provision	Section 8 (6) Data fiduciary to notify Data Protection Board.	Article 33 Notification of a personal data breach to the supervisory authority Article 34 Communication of a personal data breach to the data subject.	Subpart D— Notification in the Case of Breach of Unsecured Protected Health Information Section 164.404 Notification to individuals. Section 164.406 Notification to the media Section 164.408 Notification to the Secretary. Section 164.410 Notification by a business associate

Discussion

Based on the comparison provided in the table (Table 1), the Information Technology Act, 2000 (IT Act) and Digital Personal Data Protection Act, 2023 (DPDPA) lack specific provisions in comparison to Health Insurance Portability and Accountability Act, 1996 and GDPR. Some of these have been highlighted and discussed in the section.

Health Data Protection

- HIPAA includes extensive provisions specifically addressing the protection of health information, including definitions of health information, requirements for safeguarding electronic protected health information, and restrictions on its use and disclosure.
- GDPR also includes provisions for the protection of health data under its broader framework, ensuring that such data receives special protection due to its sensitive nature.
- In contrast, the Information Technology Act and DPDPA do not have explicit provisions specifically tailored to the protection of health data. While they may cover aspects of data protection more broadly, they lack the detailed and specialized regulations found in HIPAA and GDPR concerning health information.

Consent

- GDPR and DPDPA emphasize the importance of obtaining explicit, informed, and unambiguous consent from data subjects for the processing of their personal data.

- HIPAA, while not explicitly focusing on consent, provides detailed requirements for the use and disclosure of protected health information, which may include obtaining patient consent in certain situations.
- The Information Technology Act and DPDPA do not have specific provisions comparable to GDPR regarding the detailed requirements for obtaining consent, particularly in the context of personal data processing.

Data Breach Notification

- GDPR and HIPAA mandate data breach notification requirements, specifying the obligations of organizations to notify supervisory authorities and affected individuals in the event of a data breach.
- The Information Technology Act and DPDPA lack specific provisions requiring organizations to notify authorities or individuals in the event of a data breach. While they may have broader provisions related to data security, they do not include detailed requirements for breach notification comparable to GDPR and HIPAA.

Rights of Data Subjects

- GDPR and DPDPA grant extensive rights to data subjects, including the right to access, rectification, erasure, and the right to object to processing.
- HIPAA provides certain rights related to accessing and amending health information but does not offer the same level of granularity as GDPR and DPDPA.
- The Information Technology Act does not specifically outline detailed rights of data subjects comparable to GDPR and DPDPA. While it may include broader provisions related to data protection, it lacks the specific rights and procedures for data subjects found in GDPR and DPDPA.

Conclusion

There are numerous risks and threats developing every day and the current legislation governing privacy of data of any kind in India are not specifically framed to deal with privacy, confidentiality and security of medical records, thereby rendering EHRs susceptible to high level risks and threats, of which one of them is cyber-attack. Cyber-attack is not a merely fictitious event anymore; the incidences are occurring frequently and legal machinery to handle such incidences is not properly equipped with requisite provisions. Furthermore, the authorized government body responsible to deal with such occurrences is CERT-In established under section73 of Information Technology Act, 2000 in 2004 set up to prevent cyber-attacks, issue guidelines, advisories and enforce emergency measures as well. However, it is also important to note that guidelines, advisories issued by CERT-In do not possess enforcing characteristics. The legislative measures which have been introduced through the new Digital Personal Data Protection Act, 2023 last year, also does not consist of provisions directed at protection of health data specifically nor it have been addressed in the current legislation, i.e. Information Technology Act, 2000 or succeeding Amendment in 2008. Recurring attacks, threats and risks are putting our health data at stake and lessons must be learnt not only from the recent cyber-attack on AIIMS hospital or Indian Council for Medical Research database but subsequent incidences occurring internationally as well. Furthermore, the country's policies require not just punitive but a preventive legislation as well, which can be attained through making provisions of Electronic Health Records Standards, 2016 mandatory for all health service providers including private sector. Besides, legal machinery, there is also an utmost necessity of training among clinicians and Law enforcement personnel to be aware of issues concerning cybersecurity and procedure thereby required to be complied with in case of occurrence of such event; and absence of provisions of sensitive records database management has made it only harder to achieve the primary objective of protecting privacy individual's data.

Abbreviations

HER: Electronic Health Records
IT Act: Information Technology Act.
DPDPA: Digital Personal Data Protection Act.
NCP: National Cybersecurity Policy
GDPR: General Data Protection Regulation
HIPAA: Health Insurance Portability and Accountability Act (Privacy Rule)

Acknowledgement

Nil.

Author Contributions

Ms. Niharika Raizada initiated the idea of research on preservation of health information privacy and

analysis of the legal framework. Prof. (Dr.) Mamata Biswal was responsible for analysis and reviewing the work.

Conflict of Interest

None.

Ethics Approval

Not applicable.

Funding

Nil.

References

1. Acharya B. The four parts of privacy in India. Economic and Political Weekly. 2015 [cited 2024 Jul 2];50(22):32–8. Available from: https://www.jstor.org/stable/24482489; Availablefrom: http://journals.sagepub.com/doi/10.1177/1550147719889591; Available from: https://linkinghub.elsevier.com/retrieve/pii/S1110866520301365; Available from: https://linkinghub.elsevier.com/retrieve/pii/S1110866520301365.
2. Bhatia D. A comprehensive review on the cyber security methods in Indian Organisation. ijasca [Internet]. 2022 Apr 20;14(1):103–24. Available from:http://ijasca.zuj.edu.jo/PapersUploaded/2022.1.8.pdf.
3. Bhatia G. State surveillance and the right to privacy in India: a constitutional biography. Rochester, NY; 2015. Available from: https://papers.ssrn.com/abstract=2605317.
4. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018 Jul;113:48–52. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0378512218301658.
5. Electronic Health Records Standard. 2016a. Available from: https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf.
6. Electronic Health Records Standard. 2016b. Available from: https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf.
7. Electronic Health Records Standard. 2016c. Available from: https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf.
8. Electronic Health Records Standard. 2016d. Available from: https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf.
9. General Data Protection Regulation (GDPR) – official legal text. General Data Protection Regulation (GDPR). Available from: https://gdpr-info.eu/.
10. Gobind v. State of Madhya Pradesh (1975) 2 SCC 148.
11. Hakak S, Khan WZ, Imran M, Choo KKR, Shoaib M. Have you been a victim of covid-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. IEEE Access. 2020 [cited 2024 Mar 23];8:124134–44. Available from: https://ieeexplore.ieee.org/document/9129700.
12. HIPAA. 0991–AB08 Feb 26, 2001. Available from: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf.
13. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules. Sect. Rule 3 2011a p. 2. Available from: https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=GSR313E_10511(1)_0.pdf.
14. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, PART II-SEC. 3(i) § Rule 3 (2011b). https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=GSR313E_10511(1)_0.pdf.
15. Information Technology Act. 21. Sect. 43A Jun 9, 2000a p. 19–20. Available from: https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf.
16. Information Technology Act. 21. Sect. 43A Jun 9, 2000b p. 19–20. Available from: https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf.
17. Information Technology Act. 21. Sect. 43A Jun 9, 2000c p. 19–20. Available from: https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf.
18. Information Technology Act. 21. Sect. 43A Jun 9, 2000d p. 19–20. Available from: https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf.
19. K.S. Puttuswamy v. Union of India (II), WP (C) 494/2012.
20. K.S. Puttuswamy v. Union of India, Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161.
21. K.S. Puttuswamy vs Union of India, Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161.
22. Kaplan B. How should health data be used? Privacy, secondary use, and big data sales. SSRN Journal. 2014 [cited 2024 Mar 23]; Available from: http://www.ssrn.com/abstract=2510013.
23. Kaplan B. Seeing through health information technology: the need for transparency in software, algorithms, data privacy, and regulation*. Journal of Law and the Biosciences. 2020 Jul 25 [cited 2024 Mar 23];7(1):lsaa062. Available from: https://academic.oup.com/jlb/article/doi/10.1093/jlb/lsaa062/5918487.
24. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. 2021a Jul [cited 2024 Mar 23]; 22(2):177–83.
25. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. 2021b Jul [cited 2024 Mar 23]; 22(2):177–83.
26. Kharak singh v. State of Uttar Pradesh [Internet]. Global Freedom of Expression. [cited 2024 Jul 2]. Available from: https://globalfreedomofexpression.columbia.edu/cases/singh-v-uttar-pradesh/.
27. Kharak singh v. State of Uttar Pradesh. Global Freedom of Expression. [cited 2024 Jul 2]. Available

from: https://globalfreedomofexpression.columbia.edu/cases/singh-v-uttar-pradesh/.
28. Kharak singh v. State of Uttar Pradesh. Global Freedom of Expression. [cited 2024 Jul 2]. Available from: https://globalfreedomofexpression.columbia.edu/cases/singh-v-uttar-pradesh/.
29. Kharak singh v. State of Uttar Pradesh. Global Freedom of Expression. [cited 2024 Jul 2]. Available from: https://globalfreedomofexpression.columbia.edu/cases/singh-v-uttar-pradesh/.
30. M.P. Sharma v. Satish Chandra 1954 AIR 300, 1954 SCR 1077, AIR 1954 Supreme Court 300.
31. M.P. Sharma v. Satish Chandra 1954 AIR 300, 1954 SCR 1077, AIR 1954 Supreme Court 300.
32. Mr. Xv. Hospital Z, AIR 1995 SC 495.
33. Muthuppalaniappan M, Stevenson K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. Int J Qual Health Care. 2021 Feb 20;33(1):mzaa117.
34. Price WN, Kaminski ME, Minssen T, Spector-Bagdady K. Shadow health records meet new data privacy laws. Science. 2019 Feb 1;363(6426):448–50. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6417878/.
35. R. Rajagopal v. State of Tamil Nadu. Global Freedom of Expression. Available from: https://globalfreedomofexpression.columbia.edu/cases/r-rajagopal-v-state-of-t-n/.
36. R. Rajagopal v. State of Tamil Nadu. Global Freedom of Expression. Available from: https://globalfreedomofexpression.columbia.edu/cases/r-rajagopal-v-state-of-t-n/.
37. R.M. Malkani v. State of Maharashtra (1973) 1 SCC 471, 476.
38. Rubí JNS, Gondim PRDL. Interoperable internet of medical things platform for e-health applications. International Journal of Distributed Sensor Networks. 2020 Jan; 16(1):155014771988959.
39. Seqrite Annual Threat Report 2021. Available from: https://www.seqrite.com/seqrite-annual-threat-report-2021#dflip-df_book_full/1/.
40. Škiljić A. Cybersecurity and remote working: Croatia's (Non-)response to increased cyber threats. IntCybersecur Law Rev. 2020 Oct 1;1(1):51–61. Available from: https://doi.org/10.1365/s43439-020-00014-3.
41. The Digital Personal Data Protection Act, 2023. 22 of 2023. Sect. Preamble Aug 11, 2023 p. 1. Available from: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
42. The Digital Personal Data Protection Act, 2023. 22 of 2023. Sect. 5 Aug 11, 2023 p. 4. Available from: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
43. The Digital Personal Data Protection Act, 2023. 22 of 2023. Sect. 6 Aug 11, 2023 p. 5. Available from: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
44. The Digital Personal Data Protection Act, 2023. 22 of 2023. Sect. 7 Aug 11, 2023a p. 6. Available from: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
45. The Digital Personal Data Protection Act, 2023. 22 of 2023. Sect. 7 Aug 11, 2023b p. 6. Available from: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
46. The Digital Personal Data Protection Act, 2023. 22 of 2023. Sect. 10 Aug 11, 2023a p. 8. Available from: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
47. The Digital Personal Data Protection Act, 2023. 22 of 2023. Sect. 10 Aug 11, 2023b p. 8. Available from: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
48. The Digital Personal Data Protection Act, 2023. 22 of 2023. Sect. 2 (s) Aug 11, 2023b p. 3. Available from: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.
49. Wiggins and Froome medical records released by 'Russian hackers'. BBC News. 2016 Sep 15; Available from: https://www.bbc.com/news/world-37369705.