INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions ofthe authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsever for any consequences for any action taken by anyone on the basis of information in theJournal.

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

SAFEGUARDING PATIENT PRIVACY IN INDIA: LEGAL CHALLENGES AND SOLUTIONS IN ELECTRONIC HEALTH RECORDS.

AUTHORED BY - ELEENA ANIL VADAKKEKARA
Student- Master Of Law (Intellectual Property And Trade Laws)
School Of Law
Christ (deemed to be) University, Bengaluru, India

ABSTRACT:

The rapid adoption of Electronic Health Records (EHRs) in India's healthcare system has raised significant concerns about the protection of patient privacy and data security. This research examines the current legal landscape, highlighting gaps in existing frameworks such as the Information Technology Act, 2000, and the Indian Medical Council Act, 1956. It evaluates emerging regulations like DISHA, 2018, and the Personal Data Protection Bill, 2019, identifying challenges posed by vague guidelines and weak enforcement. Through comparative analysis with legal frameworks from the US, EU, and Australia, the paper explores best practices and legal innovations in safeguarding EHRs. Key recommendations include strengthening cyber security measures, enforcing data retention protocols, and harmonizing consent frameworks. The study underscores the urgent need for robust legislative reforms to secure sensitive health information and ensure efficient digital healthcare delivery in India.

Keywords: Electronic Health Records, patient privacy, cyber-security, legal framework, DISHA, data protection, healthcare innovation.

INTRODUCTION

Electronic Health Records (EHRs) are becoming an essential component of contemporary medical systems as a result of the digital revolution in healthcare, which has brought new methods for handling and storing patient data. EHRs allow for quicker access to medical history, fewer paperwork requirements, and better patient care, among many other advantages. However, the move to digital records also brings up important privacy issues for patients, particularly in developing nations like India where legal protections are still being developed.

 ISSN: 2582-6433

Unauthorised access, misuse, and breaches of sensitive health data could potentially damage patients if they are not well protected.

In India, the Constitution guarantees a right to privacy under Article 21 (as recently recognized by the Supreme Court in its historic judgment in ***Justice K.S. Puttaswamy (Retd.) v. Union of India case***. However, current legislation does not offer detailed and strict support for the protection of medical data. The Information Technology Act 2000 and The Indian Medical Council Act, 1956 have little provisions around protection of digital health information and lack the ability to deal with new problems that come when you put healthcare on digital mode.

So, new legal measures like Digital Information Security in Healthcare Act (DISHA), 2018 and the Personal Data Protection Bill (PDPB), 2019 have been born to deal with such challenges. But they run afoul of unclear rules, low penalties and no teeth for enforcement, meaning that most patient data leaks still have workarounds. The absence of unambiguous consent mechanisms and a lack of patient knowledge about their privacy rights only increases the risk.

The research paper studies the legal challenges to patient privacy in the area of EHRs that India faces within its healthcare system. This paper benchmarks India legislation against global standards (such as the Health Insurance Portability and Accountability Act) in the U.S. and (General Data Protection Regulation) GDPR in European Union — to establish a set of guidelines for legislating on digital health records in future. It aims to provide a legal framework for the safe handling of EHRs, respecting patient privacy as a fundamental right.

RESEARCH QUESTIONS

i. What are the current legal frameworks in India that regulate patient privacy and electronic health records (EHRs).
ii. What are the primary legal obstacles that patients encounter in India with respect to privacy in the context of EHRs?
iii. In what way do these frameworks correspond to international standards, such as those in Australia the United States and the European Union?
iv. How can legal safeguards for patient privacy be enhanced in India's digital healthcare environment?

 ISSN: 2582-6433

RESEARCH OBJECTIVES:-

i. To conduct an analysis of the existing legal provisions concerning EHRs in India, with a view of identifying any gaps or deficiencies.
ii. To emphasise the most effective practices, a comparative analysis of India's legal framework with those of the United States, European Union, and Australia will be conducted.
iii. To examine the legal challenges resulting from unauthorised access, data breaches, and other risks associated with electronic health records (EHRs).
iv. To suggest practical recommendations for the reform of India's legal system in order to improve the protection of patient privacy

RESEARCH METHODOLOGY:

This research employs a doctrinal and comparative legal research approach to analyze the legal challenges associated with protecting patient privacy in India's Electronic Health Records (EHR) system. The doctrinal analysis involves examining existing laws such as the Information Technology Act, 2000 (Sections 43A and 72A), the Indian Medical Council Act, 1956, the proposed Digital Information Security in Healthcare Act (DISHA), 2018, and the Personal Data Protection Bill (PDPB), 2019. A comparative legal analysis is conducted by evaluating India's regulatory framework against international standards, including the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in the European Union, and Australia's My Health Records Act, 2012. This comparison highlights best practices, such as HIPAA's requirements for breach notifications, GDPR's consent-based data processing, and Australia's patient-centered data control model.

A descriptive and analytical approach is used to identify major challenges, including unauthorized access, phishing attacks, insider threats, and weak enforcement mechanisms. The prescriptive aspect of the research suggests legal reforms such as strengthening cybersecurity laws, enforcing stricter data retention policies, harmonizing existing regulations, and improving consent frameworks.

The study follows the Bluebook citation style (20th edition) and primarily relies on legal statutes, case laws, and government reports as primary sources. It also incorporates secondary

 ISSN: 2582-6433

sources, including academic articles and comparative legal studies, to ensure a well-rounded analysis of the legal issues in India's EHR system.

ELECTRONIC HEALTH RECORDS:

According to the American Health Information Management Association (AHIMA), the digital form of medical records is classified into Electronic Medical Records (EMRs-used to document patient enrolment, billing, scheduling, and quality-of-care monitoring); Electronic Health Records (EHRs- a longitudinal electronic document prepared by doctors in any type of healthcare facility that contains patient health data including the patient's treatment history, demographics, test results, status of illnesses, and medical history etc.);and Personal Health Records(PHRs-compiles important data about patients and their relatives.)[1].

Although the Electronic Medical Record (EMR) system has many benefits, there are also legal concerns related to confidentiality and privacy violations. The challenges encompass inadequate planning, insufficient accessibility, limited technical resources, data migration, disruptions to worker workloads, and a scarcity of cost- effective software. This paper covers the problems, legal consequences, preventive mechanisms, medical ethics, and best practices for EMR implementation in India.

The Advantages and Ethical-Legal Concerns of Electronic Health Records (EHR) in Modern Healthcare

Electronic Health Records (EHRs) have transformed healthcare by improving patient data management, enhancing accessibility, and streamlining administrative tasks. They enable seamless data exchange among healthcare providers, ensuring that patient information such as medical history, allergies, and billing details is well-organized and readily available. Unlike traditional paper-based records, which are prone to errors and difficult to manage[2], EHRs provide accurate and standardized documentation, minimizing medical errors and enhancing patient safety[3]. Additionally, these digital systems support better decision-making by offering evidence-based recommendations to physicians, improving overall healthcare outcomes.

---

[1] *E-record, e-liability. Addressing medico-legal issues in electronic records. Vigoda M, Dennis JC, Dougherty M. https://pubmed.ncbi.nlm.nih.gov/18939674/ J AHIMA. 200879:48–52*

[2] *Aranya Nath, Gautami Chakravarty & Saumya Goel, Legal Regulation of Digitising and Outsourcing Medical Records Department in India, 9 NUJS J. REGUL. STUD. 85 (July-September 2024)*

[3] *Abha Agrawal, Medication Errors: Prevention Using Information Technology Systems, 67 BR J CLIN PHARMACOL 681 (2009).*

 ISSN: 2582-6433

One of the most significant advantages of EHRs is their ability to enhance administrative efficiency and reduce costs. By eliminating the need for physical storage, refiling, and transcription, EHRs streamline workflow processes, allowing healthcare providers to focus more on patient care[4]. Cloud-based storage solutions further improve accessibility, enabling authorized personnel to update and retrieve patient records securely from different locations[5]. EHRs also support public health initiatives by facilitating disease surveillance and epidemiological research, as anonymized data can be used to track health trends and allocate resources effectively. The integration of EHRs across healthcare systems strengthens healthcare coordination, leading to improved treatment planning and patient management[6].

Despite these benefits, the implementation of EHRs presents ethical and legal challenges. Patient autonomy must be respected, as individuals have the right to decide whether their medical data should be stored electronically. However, in emergency situations, healthcare providers may proceed with registration without explicit consent to ensure timely treatment[7]. Confidentiality and data privacy are critical concerns, as unauthorized access or data breaches can compromise sensitive patient information. While confidentiality must be maintained, certain infectious diseases must be reported to public health authorities as required by law[8]. Ethical principles such as beneficence and non-maleficence also come into play[9], as the use of EHR data for research should enhance healthcare services while ensuring patient identities remain protected[10].

From a legal perspective, EHR systems must comply with stringent data protection laws to prevent cybersecurity threats and unauthorized access. Cybersecurity risks, including hacking and data theft, pose significant challenges, making it essential to implement strong encryption and authentication protocols. Additionally, medical errors resulting from incorrect

[4] *Singh, S., Pankaj, B., Nagarajan, K., P. Singh, N., & Bala, V. (2022). Blockchain with cloud for handling healthcare data: A privacy-friendly platform. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2022.04.910*
[5] *IBID*
[6] *Keshta, I., & Odeh, A. (2020). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. https://doi.org/10.1016/j.eij.2020.07.003*
[7] *A. Gaur, A. Singh, A. Nautiyal, et al.: A deep neural network based virtual memory analysis for malware detection at hypervisor-layer. International Conference on Advances in Intelligent Computing and Applications (AICAPS), Kochi, India. 2023, 10.1109/AICAPS57044.2023.1007434*
[8] *Taylor RM: Ethical principles and concepts in medicine. Handb Clin Neurol. 2013, 118:1-9. 10.1016/B978-0-444-53501-6.00001-9*
[9] *Ozair FF, Jamshed N, Sharma A, Aggarwal P: Ethical issues in electronic health records: a general overview. Perspect Clin Res. 2015, 6:73-6. 10.4103/2229-3485.153997*
[10] *Schyve PM: Patient rights and organization ethics. The Joint Commission perspective. Bioethics Forum. 1996, 13-20.*

 ISSN: 2582-6433

documentation or system failures can lead to malpractice claims, highlighting the need for regular system updates, staff training, and quality control measures. Regulatory compliance is another crucial aspect, with laws such as the Data Protection Act of 2023 in India imposing strict penalties for unauthorized access to patient data. Healthcare institutions must enforce security policies, ensure proper data retention, and prevent fraudulent billing practices to maintain legal and ethical standards.

Electronic Health Records Recognition in India

Current Regulatory Framework

India lacks a unified regulatory framework for Electronic Health Records (EHR). Presently, EHRs are governed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (IT Rules, 2011)[11]. These rules classify health data as sensitive personal information and require a notice-and-consent framework for its collection, use, disclosure, transfer, and deletion. However, these provisions apply only to corporate healthcare providers, leaving a significant portion of the sector unregulated[12]. Additionally, the rules do not address interoperability, which is crucial for an effective EHR system[13].

The Clinical Establishments (Registration and Regulation) Act, 2010, mandates EHR adoption by healthcare providers, but its enforcement remains weak. The Ministry of Health and Family Welfare (MoHFW) has introduced voluntary EHR standards [14]covering patient identifiers, data exchange protocols, and functional requirements, supported by accreditation bodies such as the National Accreditation Board for Hospitals (NABH[15]).

Legal Recognition of Medical Records

The "Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002" require physicians to maintain medical records of indoor patients for three years. The "Limitation Act of 1963" mandates the preservation of outpatient records for two years, while

[11] *the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*
[12] *Kaur, h. (2020, August). Electronic Health Records in India: Legal Framework and Regulatory Issues. Just a moment... https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3686303*
[13] *Clinical Establishments (Central Government) Rules, 2012 (India), available at http://clinicalestablishments.gov.in/WriteReadData/386.pdf,(last accessed on 1 Jan 2025)*
[14] *electronic health record standards for india. (n.d.). ministry of health and family welfare. https://mohfw.gov.in/?q=basicpage/electronic-health-record-ehr-standards-india-2016*
[15] *Ibid*

 ISSN: 2582-6433

the "Consumer Protection Act of 1986" requires inpatient and surgical records to be retained for three years. Additional regulations, such as the "Pre-Conception and Prenatal Diagnostic Techniques (PCPNDT) Act of 1994," impose document retention requirements. Despite these regulations, India lacks an overarching law ensuring uniform medical data protection.

Existing Legal Gaps in Medical Data Security

Fragmented Framework: The Clinical Establishments Act, 2010, which mandates licensing and regulation of healthcare institutions, has not been uniformly enforced across all states. Additionally, the Information Technology (IT) Act, 2000, and IT Rules, 2011, provide only limited protections, primarily applying to corporate healthcare entities without strict penalties for non-compliance.

Lack of Mandatory Breach Notification: Unlike international models such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, India lacks a robust system for reporting privacy breaches and imposing strict penalties for data mishandling. Countries like Australia have expanded their privacy laws to include stringent health data protection measures, while India's approach remains fragmented.

Proposed/Emerging Frameworks: DISHA and NDHB

To address these gaps, The two main legislative framework were introduced in India to regulated HER- the Personal Data Protection Bill, 2019 (PDPB) and the Digital Information Security in Healthcare Act, 2018 (DISHA). Although the protection of health data is the fundamental objective of both systems, their techniques and regulatory purviews differ.

- **DISHA**:- The Digital Information Security in Healthcare Act of 2018 (**DISHA**) is a landmark initiative by the Indian government (*The Ministry of Health and Family Welfare-**MoHFW***) aimed at securing healthcare data in the digital age.

  DISHA primarily focuses on the privacy, confidentiality, and security of digital health data while ensuring the standardization and regulation of its collection, storage, transmission, and usage.[16]The Act complements broader data protection measures, such as the Personal Data Protection Bill (**PDPB**) of 2019, but is uniquely tailored to healthcare data.

  A core feature of DISHA is the establishment of centralized regulatory authorities: the

[16] *Digital Information Security in Healthcare Act, 2018, Ministry of Health & Family Welfare, https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf (last visited Sept. 12, 2024).*

 ISSN: 2582-6433

National Electronic Health Authority (**NEHA**) [17]and State Electronic Health Authorities (**SEHA**)[18]. These bodies are empowered with quasi-judicial authority, akin to civil courts, to address disputes and ensure compliance with digital health data protocols. DISHA also mandates the creation of health information exchanges, overseen by a Chief Health Information Executive, to facilitate secure data transmission between clinical establishments.

The Act prohibits the commercial use of digital health data, forbidding its disclosure to entities like insurance companies, employers, and pharmaceutical firms, regardless of whether the data is identifiable or anonymized. This ensures that patient health data is not exploited for financial or non-healthcare purposes.

DISHA provides for stringent penalties for data breaches, categorizing them as "breaches"[19]

or "serious breaches"[20] based on intent where a serious breach could result in *Imprisonment Of Three To Five Years Or Fines Of Up To Five Lakh Rupees*. The Act also mandates that patients be informed of any data breaches and allows them to claim compensation for damages caused.

It expressly prohibits commercial use of digital health data[21].The Act emphasizes patient consent, ensuring that health data cannot be stored, accessed, or transmitted without the express written consent of the patient. By establishing a regulatory framework for digital health data, DISHA is a critical step toward safeguarding patient privacy in India's evolving digital healthcare landscape.

DISHA incorporates the following provisions to safeguard the confidentiality of digital health data:-Under Section 22(1)(e), the NEHA is tasked with establishing protocols for the transmission and receipt of digital health data across borders, along with standards for physical, administrative, and technical safeguards to ensure the privacy and confidentiality of data during transmission.

- **Personal Data Protection Bill (PDP Bill):-** The Personal Data Protection (PDP) Bill, introduced in December 2019 in the Indian Parliament, represents a significant legislative step toward safeguarding individual privacy and data security in India. It was initially drafted by a committee led by **Justice B.N. Srikrishna** in July 2018 and was

[17] *Digital Information Security in Healthcare Act (DISHA), 2018, §5*
[18] *Digital Information Security in Healthcare Act (DISHA), 2018, §7*
[19] *Section 37 of DISHA*
[20] *Section 38 of DISHA*
[21] *Digital Information Security in Healthcare Act (DISHA), §38(d)*

 ISSN: 2582-6433

later revised in 2019. Currently under review by a Joint Select Committee, the Bill is anticipated to be enacted soon. It establishes a comprehensive framework for data protection, including the creation of a Data Protection Authority of India, which will oversee and enforce the law's provisions.

- **Objective**: The PDP Bill aims to safeguard personal data, drafted to address the growing concerns over data misuse and privacy breaches in India.
- **Data Protection Authority**: Establishes the **Data Protection Authority of India**, responsible for overseeing the implementation and enforcement of the law.

DISHA and the PDPB: A Comparative Analysis

Both the Digital Information Security in Healthcare Act (DISHA) and the Personal Data Protection Bill (PDPB) acknowledge health data as sensitive and impose strict controls to ensure its confidentiality and security. A key similarity between the two is their reliance on a consent-based framework, requiring individuals (data principals) to provide explicit consent before their health data can be collected, processed, or shared.

However, there are notable differences between DISHA and the PDPB, particularly in terms of consent requirements. DISHA enforces stricter consent mandates, requiring approval at every stage of data handling, including its generation, storage, transmission, and disclosure. It imposes stringent restrictions on data use and retention (Sections 28, 29). In contrast, while the PDPB also emphasizes consent, it permits broader exceptions, allowing data processing without consent in medical emergencies, for legal compliance, and for "reasonable purposes" such as preventing illegal activities or ensuring network security (Sections 12, 14).

Ownership and rights related to health data also differ between the two frameworks. DISHA explicitly grants data principals extensive rights, including privacy, security, and the ability to refuse or grant consent. It also mandates transparency regarding who accesses the data and restricts pharmaceutical companies from exploiting health data without consent. Furthermore, DISHA requires data to be anonymized or de-identified when used for public health purposes (Section 29). On the other hand, the PDPB does not explicitly define health data ownership in as much detail but permits data processing for a wider range of purposes, including some without consent, such as commercial and operational uses (Section 14).

 ISSN: 2582-6433

The regulatory frameworks governing these laws are also distinct. DISHA is overseen by the National Electronic Health Authority (NeHA), which focuses specifically on digital health data compliance (Clause 4). To the contrary, the PDPB falls under the jurisdiction of the Data Protection Authority of India (DPA), which regulates all types of personal data, including health information (Clause 41).

Another major point of difference is the scope of non-consent-based data processing. DISHA limits such processing strictly to specific public health and research purposes, provided the data is anonymized (Section 29). This ensures individual consent remains a priority, significantly restricting the broader use of health data. In contrast, the PDPB permits a much wider range of non-consent-based data processing, including for law enforcement, credit assessment, and network security, thereby accommodating various commercial and operational needs (Section 14).

COMPARATIVE ANALYSIS: [EU, USA, AUSTRALIA]

EU (European Union) Position

Data protection laws are designed to regulate 'personal data'—information about individuals or 'data subjects'—handled by 'data controllers' and 'data processors'. Not all information about a person is subject to these regulations; only data that impacts an individual's privacy is considered 'personal'.

3.1.(01) Responsibilities of Controllers and Processors

i. Data Controllers: Responsible for determining the purposes and means of processing personal data. They are accountable for ensuring data is processed in compliance with legal requirements.

ii. Data Processors: Act on behalf of data controllers and are subject to similar strict conditions as controllers. They must also ensure that appropriate technical and organizational measures are in place to protect personal data and are monitored by controllers.

3.1.(02) EU Data Protection Directive

Foundation: The Directive forms the basis of data protection laws in EU Member States and establishes eight core principles for data protection.

 ISSN: 2582-6433

3.1.(03) Core Principles includes:

a. Lawful Processing: Data must be processed fairly and lawfully.
b. Specified Purposes: Data should be collected for specified, legitimate purposes and not used for incompatible purposes.
c. Data Minimization: Only data necessary for the intended purpose should be collected.
d. Accuracy: Data should be accurate and kept up to date.
e. Storage Limitation: Data should not be kept longer than necessary for the purpose for which it was collected.
f. Integrity and Confidentiality: Data must be protected against unauthorized access and processing.
g. Accountability: Data controllers must ensure compliance with these principles and demonstrate adherence.
h. Technical and Organizational Measures: Both controllers and processors must implement suitable measures to safeguard data.

3.1.(04) Data Transfer and Adequacy

- Within the EU: Data transfers between Member States are regulated under the Directive to ensure a uniform level of protection.
- Outside the EU: Transfers to third countries are evaluated based on the adequacy of protection in the recipient country, considering factors such as the nature of data, purpose, and duration of processing.

- I v. Finland (2008)[22]: The European Court of Human Rights (**ECtHR)** highlighted the significance of protecting sensitive health data. The case involved unauthorized disclosure of an individual's HIV status by an eye clinic, underscoring the need for stringent confidentiality measures. The ECtHR emphasized the importance of safeguarding sensitive information and ensuring confidentiality.

The EC Data Protection Directive sets out a comprehensive framework for the protection of

[22] *I v. Finland, Application No. 20511/03: 2008 ECHR 623 (reiterating the Court's earlier ruling in Z v. Finland, (1988) 25 EHRR 371, that an individual's ability to exercise their fundamental right to respect for their private and family life, as protected by Article 8 of the Convention on Human Rights, depends on the protection of personal data, particularly medical data. or her right to respect for her private and family life, as provided by Article 8 of the European Convention on the Protection of Health Information, which is a fundamental principle in the legal systems of all Contracting Parties to the Convention.. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention).*

 ISSN: 2582-6433

personal data within the EU, establishing eight data protection principles for states implementing the Directive [23] and requiring both data controllers and processors to adhere to strict standards of data handling. The principles established by the Directive aim to ensure that personal data is processed lawfully, kept secure, and only used for its intended purpose. The Directive also provides guidance on data transfers and highlights the need for robust protections for sensitive information, as demonstrated by key case law such as I v. Finland.

American Position

The United States has taken a sectoral approach to data protection, meaning it lacks a comprehensive federal law governing personal data across all sectors. However, healthcare privacy and security are addressed by key legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

3.2.(01) HIPAA (1996)*:*

It is the primary law that sets national standards for the protection of health information. It applies to "covered entities," which include healthcare providers, health plans, and healthcare clearinghouses, as well as their business associates who handle protected health information (PHI) on their behalf. The law is designed to protect "individually identifiable health information" (PHI), which includes demographic data related to an individual's physical or mental health, medical treatments, and payments.

HIPAA consists of several key rules:

1. *Privacy Rule*: Establishes standards for the use and disclosure of PHI, protecting patients' privacy while allowing information sharing for treatment, payment, and healthcare operations without authorization. It mandates that covered entities disclose PHI to individuals or their representatives upon request and to the Department of Health and Human Services (HHS) for compliance purposes.
2. *Security Rule*: Protects Electronic Protected Health Information (ePHI) by establishing standards for the confidentiality, integrity, and availability of data held or transferred electronically. It requires covered entities to implement

[23] *UK Data Protection Act, 1998, Schedule I, c. 29 of 1998, Acts of Parliament, 1998 (UK). (Data Protection Directives are part of the Council of Europe's attempts to harmonise national laws on data protection in its 1973 and 1974 resolutions).*

 ISSN: 2582-6433

administrative, technical, and physical safeguards to protect ePHI from reasonably anticipated threats and unauthorized disclosures.

3. *Breach Notification Rule:* Requires covered entities and business associates to notify affected individuals, HHS, and sometimes the media in the event of a data breach involving unsecured health information. This rule applies to impermissible uses or disclosures that compromise the security or privacy of PHI.[24]

3.2.(02) HITECH (2009) :

Purpose: It was enacted to enhance the adoption and meaningful use of Electronic Health Records (EHRs) and to strengthen existing regulations under the Health Insurance Portability and Accountability Act (HIPAA). The Act promotes EHR adoption by establishing incentive programs for healthcare providers, expands HIPAA's Privacy and Security Rules to cover business associates, and imposes more stringent regulations on handling electronic data.

Certification Process: Managed by the Office of the National Coordinator for Health Information Technology (ONC) and the Certification Commission for Healthcare Information Technology (CCHIT).

Requirements: EHR systems must comply with HIPAA rules, including:

→ **Confidentiality:** Database encryption and transmission mode encryption.

→ **Access Control:** Authentication mechanisms, automatic log-off, and emergency access protocols.

→ **Data Integrity:** Ensured through audit trail logs.

→ **HIPAA Compliance:** Addressing releases of information under HIPAA.[25]

Both HIPAA and HITECH have significantly influenced the development of EHRs, but their protections apply only to specific entities, leaving gaps where personal health data may not be adequately protected. Additionally, the rules do not always clearly differentiate between data in transit and data at rest, nor do they set minimum encryption standards, which has left healthcare systems vulnerable to cyber threats like ransomware attacks.

---

[24] *Purvi Nema & Riya SinhaPurvi Nema, N.U.S.R.L. and Riya Sinha, N.U.S.R.L., Privacy And Security Concerns In Electronic Health Records-A Comparative Study Between India And USA. Journal of Law and Legal Studies, 1(1). https://hcommons.org/deposits/item/hc:43075/*

[25] *The Office of the National Coordinator for Health Information Technology, Guide to Privacy and Security of Electronic Health Information, (2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-securityguide. pdf.*

 ISSN: 2582-6433

Despite these challenges, HIPAA and HITECH represent crucial steps toward securing patient data in the U.S. healthcare system. However, the lack of a unified federal approach and strong encryption requirements indicates a need for continuous updates to the framework to address evolving cybersecurity risks.

AUSTRALIAN Position.

3.3.(01) Privacy Act 1988

The Privacy Act 1988 forms the backbone of privacy protection in Australia, particularly concerning health information. It applies to both the Commonwealth public sector and the national commercial sector, including health service providers and those merely storing health data. The Act is overseen by the *Office of the Australian Information Commissioner* (OAIC) and includes rules for the collection, handling, and disclosure of health data.

Key provisions of the Privacy Act relevant to EHRs:

- Collection and Use of Health Data: Organizations are required to follow strict protocols for collecting and processing health information, ensuring it is only used for the intended purpose.
- Medical Research Guidelines: The *National Health and Medical Research Council* (NHMRC) has issued two mandatory guidelines (Sections 95 and 95A of the Act) allowing:Use of personal health information for research from Commonwealth institutions, subject to strict protocols,Handling of identifiable health information without explicit consent, provided criteria are met.
- Genetic Information Disclosure: The Act allows the disclosure of genetic information without consent if necessary for the patient's healthcare or in cases where a genetic relative's life is at significant risk (Section 95AA).

CONCLUSION & SUGGESTION.

4.1 Conclusion

The digitization of healthcare in India holds significant promise for improving patient care, expanding accessibility, and enhancing connectivity within the healthcare system. Nevertheless, it also presents substantial challenges regarding the protection of sensitive health information. Electronic Health Records (EHRs) are crucial for modernizing healthcare delivery, but their implementation in India faces hurdles due to inadequate infrastructure, legal

 ISSN: 2582-6433

frameworks, and technological preparedness.

Currently, the legal landscape is fragmented. Laws such as the Information Technology Act, 2000, and various sector-specific guidelines fall short in addressing the unique challenges posed by EHRs. While initiatives like the Digital Information Security in Healthcare Act (DISHA), 2018, and the Personal Data Protection Bill (PDPB), 2019, aim to protect digital health data, their effectiveness is compromised by weak enforcement and practical application issues. DISHA is promising in its focus on healthcare data security but suffers from vague guidelines and limited enforcement. The PDPB, though comprehensive in its approach to data protection, lacks a specific focus on healthcare data, leading to legal ambiguities and potential conflicts between different regulations.

International models offer valuable insights. The U.S., with its HIPAA regulations, enforces stringent data breach and audit trail requirements. The EU's GDPR provides global standards for data protection, including healthcare data. Australia's My Health Records Act, with its emphasis on patient empowerment and control over health data, highlights effective practices in EHR management. These models underscore the importance of standardized protocols, rigorous enforcement, and patient-centric approaches.

For India to advance, it must focus on stronger public-private sector coordination, adopt internationally recognized EHR standards, and invest in cloud-based infrastructure. Training for healthcare professionals and developing a unified regulatory framework that ensures transparency and accountability are crucial. Safeguarding patient privacy is essential for building trust in the digital healthcare system. Legal reforms, robust cybersecurity measures, and effective enforcement of existing laws are key to protecting patient privacy while leveraging the benefits of EHRs.

4.2 Suggestions For India

NEED FOR A DEDICATED LEGAL FRAMEWORK

A sector-specific healthcare data protection law is essential to provide legal certainty and prevent regulatory fragmentation. Countries like the United States have established frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, ensuring stringent regulations for health data protection. India should adopt a similar approach by

 ISSN: 2582-6433

enacting a dedicated law that governs data collection, processing, storage, and breach management in healthcare. Furthermore, harmonizing this law with existing legislation, such as the Information Technology Act, 2000, and the Right to Information Act, 2005, is crucial to avoid overlapping provisions and regulatory inconsistencies.

STRENGTHENING DATA PRIVACY AND SECURITY MEASURES

Ensuring the confidentiality and integrity of health data is fundamental to the successful adoption of EHRs. Implementing strict access control measures, such as role-based access and multi-factor authentication, will help regulate data access based on professional responsibilities. Additionally, healthcare institutions must adopt strong cybersecurity protocols, including encryption, periodic risk assessments, and workforce training to mitigate potential breaches. These measures should align with international best practices to ensure the security of electronic health information.

ESTABLISHING A DATA BREACH NOTIFICATION MECHANISM

A well-defined breach notification framework is necessary to ensure transparency and accountability. Healthcare providers should be mandated to report data breaches promptly to affected individuals, regulatory authorities, and other relevant stakeholders. The timeline and mode of disclosure should follow established global standards, such as those outlined under HIPAA. Additionally, audit trail requirements should be introduced to log and monitor all activities related to EHR access, modification, and deletion, ensuring compliance and accountability in data handling.

DEFINING DATA OWNERSHIP AND REGULATORY OVERSIGHT

Clear ownership rights over health data must be established to empower individuals in managing their personal information. Drawing from the principles of the General Data Protection Regulation (GDPR), India's legal framework should recognize patients as the primary owners of their health data, granting them explicit rights to access, correct, and transfer their records. Additionally, a centralized regulatory authority should be established to oversee EHR governance, enforce compliance, and address grievances related to data breaches or unauthorized access.

STRENGTHENING CONSENT AND PATIENT AUTONOMY

A comprehensive consent framework is essential to ensure that patients retain control over the

 ISSN: 2582-6433

use of their health data. The framework should mandate explicit and informed consent for data collection and sharing while allowing patients to withdraw consent at any stage. Furthermore, patient access to health records should be enhanced through digital platforms, enabling them to review, update, and manage their data securely. Public awareness initiatives should also be launched to educate individuals about their data rights and the mechanisms available for redressal in case of misuse.

REGULATING ETHICAL AND COMMERCIAL USE OF HEALTH DATA

While data privacy is a priority, a balanced regulatory approach should be adopted to facilitate responsible medical research and innovation. Strict ethical guidelines must be enforced to govern the use of anonymized health data for scientific research, ensuring that privacy safeguards remain intact. Additionally, policies should be introduced to regulate the commercial use of health data, preventing unauthorized monetization while allowing controlled access for public health research and policy development.

LONG-TERM STRATEGY AND GLOBAL COLLABORATION

A future-ready legal and regulatory framework must be adaptable to technological advancements and emerging privacy challenges. Regular legislative reviews should be conducted to ensure the framework remains relevant in addressing new threats and innovations in digital healthcare. Additionally, India should engage in international cooperation with regulatory bodies and global health organizations to align its policies with best practices and facilitate secure cross-border data sharing under strict compliance protocols.