



The evolving landscape of medical confidentiality and health information privacy

Muhammad Tawfeeq B¹, Subana K²

¹ Department of Law, Chettinad Academy of Research and Education, Tamil Nadu, India

² Chettinad Dental College and Research Institute, Tamil Nadu, India

Abstract

In today's increasingly digital world, the trust we place in doctors and the privacy of our health information face new challenges. The traditional promise of medical confidentiality the assurance that what patients share with their doctors remains private is being transformed by technology. Electronic health records, wearable devices, and mobile apps have shifted medical data from paper files in locked cabinets to streams of information shared across multiple systems.

This evolution raises significant ethical and legal questions. How can patients' fundamental right to privacy be protected while allowing health data to advance medical research, improve public health, and potentially save lives? The tension between personal privacy and the societal benefits of data sharing is central to this discussion. Misuse or breaches of health information not only risk harm to individuals but also undermine the essential trust that forms the foundation of the doctor-patient relationship.

Various laws and policies, from longstanding regulations to emerging frameworks, are attempting to keep pace with technological change. However, legal compliance alone is not sufficient. Protecting health information requires a broader commitment to preserving patients' dignity, autonomy, and confidence in the medical system.

This paper argues that finding the right balance is crucial: leveraging the power of health data to improve care and research without compromising privacy. It is a conversation about trust as much as it is about technology or law. In navigating this digital age, safeguarding health information is not just a regulatory obligation but a moral imperative, ensuring that patients feel secure while society benefits from the responsible use of medical data.

This research looks at how different laws and policies, from the foundational rules of the past to new regulations of the future, are trying to keep up. Ultimately, this paper argues that protecting health information is not just about following rules.

Keywords: Medical confidentiality, health data privacy, electronic health records (EHR), Indian law, digital personal data protection act (DPDP), medical council of India, patient rights, data protection

Introduction

The sanctity of the doctor-patient relationship is built on a foundation of trust, where a patient can openly share sensitive information with their healthcare provider, confident that it will be held in strict confidence. This principle of medical confidentiality has been a cornerstone of medical ethics for centuries. However, the advent of technology has fundamentally altered how this information is collected, stored, and shared. In India, a country rapidly embracing digital healthcare initiatives, the privacy of health records has emerged as a critical concern. While digitization promises improved efficiency and better health outcomes, it also exposes a patient's most private data to new risks, from accidental breaches to malicious cyber-attacks and secondary use for commercial purposes. This paper explores the journey of health data privacy in India, from its ethical roots to its contemporary legal challenges.

Medical confidentiality and health information privacy are key principles of modern healthcare. They stem from the ethical duty of healthcare providers to protect sensitive patient information. Confidentiality means that medical professionals must not disclose information shared by patients without their consent. Health information privacy broadens this idea to include data protection, security, and control over personal health details. These principles help ensure that patients feel secure sharing important information with doctors. This trust enables accurate diagnosis, effective treatment, and ongoing care.

Historically, breaches of confidentiality were mostly personal or verbal. With the rise of electronic health records, telemedicine, and digital health technologies, the scope of health information privacy has grown significantly. Patients' health data are now stored, shared, and processed electronically. This shift raises the risk of unauthorized access, misuse, and breaches. As healthcare delivery becomes more complex and relies more on technology, the legal and ethical rules governing medical confidentiality must change to meet new challenges.

Statement of the problem

Despite the push for a digital healthcare ecosystem, India lacks a specific, comprehensive law dedicated to the protection of health data. The absence of a robust legal framework creates a vacuum where patient data is vulnerable. Current regulations are fragmented and often insufficient to address the complexities of a digital environment. This legal ambiguity can lead to:

Inadequate Protection: Patient data is at risk from unauthorized access, misuse, and breaches, which can lead to social stigma, discrimination, and financial loss.

Erosion of Trust: The lack of clear privacy safeguards can make patients hesitant to share complete and honest information with their doctors, potentially compromising the quality of care.

Legal & Ethical Gaps: There is a need for clear guidelines on data ownership, consent for secondary use (e.g., research or commercial use), and accountability for data breaches.

Research questions

- How effective are the existing legal provisions and ethical guidelines in India in safeguarding the privacy and confidentiality of health information?
- What are the key technological and operational vulnerabilities in the current Indian healthcare ecosystem that pose a threat to patient data privacy?
- How has the judiciary's interpretation of the right to privacy impacted the protection of health records in India?
- What are the essential elements of a comprehensive legal framework that India needs to ensure robust protection for health information in the digital age?

Research objectives

- To critically analyse the existing legal and regulatory framework for health data privacy in India, including the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, ^[5] and the Digital Personal Data Protection Act (DPDP), 2023.
- To identify the primary challenges and security risks associated with the digitization of health records and the use of telemedicine.
- To examine significant judicial precedents that have shaped the discourse on health information privacy in India.
- To provide recommendations for a comprehensive legal and ethical framework for the protection of health data.

Literature review

The concept of medical confidentiality in India is primarily derived from common law principles and the Hippocratic Oath. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, ^[5] provide an ethical duty for registered medical practitioners to maintain patient confidentiality. However, this regulation is limited in scope, as it only applies to registered doctors and does not cover hospitals, insurance companies, or other entities that handle health data.

Recent legal developments, such as the Digital Personal Data Protection Act, 2023, represent a significant step forward. The DPDP Act, for the first time, provides a legal definition of "sensitive personal data," which includes health data. It introduces concepts like "Data Fiduciary" (the entity determining the purpose of processing data) and "Data Principal" (the individual whose data is processed). However, its effectiveness in the healthcare sector is yet to be fully realized.

Several studies have highlighted the practical challenges. A 2019 report by the Centre for Internet and Society noted the lack of a standardized system for medical record keeping in India, leading to discrepancies in data quality and security. Furthermore, with the rise of telemedicine during the COVID-19 pandemic, new vulnerabilities in data transmission and storage have emerged, as noted in the Telemedicine Practice Guidelines, 2020, which, while offering some safeguards, are not a replacement for a robust law.

Research methodology

This research will adopt a doctrinal methodology, relying on a detailed analysis of legal statutes, legislative documents, judicial pronouncements, and existing academic literature. The study will be structured as follows:

Legal Analysis: A thorough review of key Indian laws and regulations relevant to data privacy, including the DPDP Act, the Information Technology Act, 2000, and the Indian Medical Council Regulations.

Case Law Study: An in-depth examination of landmark judicial decisions to understand the evolution of the right to privacy and its application to health data.

Documentary Analysis: Review of government reports, policy papers (such as the National Health Policy), and guidelines from organizations like the Indian Council of Medical Research (ICMR) to understand the current policy landscape.

Comparative Approach: A brief comparison with established international frameworks like the General Data Protection Regulation (GDPR) of the European Union and the Health Insurance Portability and Accountability Act (HIPAA) of the United States to identify best practices.

Legal and ethical foundations

Medical confidentiality and health information privacy rely on ethical responsibilities and legal requirements. Ethical principles shape how professionals interact with patients, while laws provide enforceable rights and solutions for breaches. Together, they create a system that keeps patient information safe and holds healthcare professionals accountable.

1. ethical foundations

The ethical commitment to medical confidentiality originates from the Hippocratic Oath, which emphasizes the doctor's duty to keep patient information private. Modern medical ethics expand this idea through several key concepts:

Autonomy: Respecting patient autonomy means recognizing their right to control personal health information.

Beneficence and Non-Maleficence: Confidentiality helps maintain patient trust and prevents psychological or social harm that might come from sharing information.

Fidelity: Keeping secrets is vital for trust in the patient-doctor relationship and for the integrity of the medical field. Professional codes, like the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, ^[5] support these ethical responsibilities. They state that medical practitioners must keep information confidential unless legally required to disclose it or given patient consent.^[1]

2. Historical Evolution of Medical Confidentiality

Confidentiality in medicine has historically been informal and based on trust, relying on the integrity of professionals. As formal legal systems emerged and patient rights were defined, ethical responsibilities were slowly backed by law. Around the world, legal systems started to recognize privacy as a basic right, influenced by human rights agreements and constitutional protections.

In the United States, HIPAA (1996) set strict rules for protecting patient data, standardizing electronic health records, and requiring privacy measures.^[1]

In Europe, the GDPR (2018) classified health data as sensitive personal information, demanding explicit consent and secure management.^[2]

India's approach has evolved alongside these global standards, combining traditional ethics with legal measures to tackle modern issues.

3. Legal Foundations

The legal acknowledgment of medical confidentiality makes ethical duties enforceable. Important legal principles include:

Right to Privacy: Recognized as a fundamental right under Article 21 of the Indian Constitution (Justice K.S. Puttaswamy v. Union of India, 2017) ^[1], this covers personal health information.

Professional Duty of Confidentiality: Defined in the Indian Evidence Act, 1872 (Sections 126–129), which protects doctor-patient communication from unauthorized disclosure in court.

Information Technology and Data Protection Laws: The IT Act, 2000, and the proposed Personal Data Protection Bill, 2019, offer legal protections for electronic health records and digital information.

Consumer Protection Law: While focused on service issues, it also ensures that healthcare providers manage patient data responsibly.

These legal foundations together create binding obligations, ensuring that breaches of confidentiality can lead to civil, criminal, or professional penalties.

4. International Comparative Perspective

A comparative look reveals an evolving global view of health information privacy:

HIPAA (USA): Requires secure storage, limited access, and patient consent for sharing health records.

GDPR (Europe): Demands clear consent for processing sensitive health data and imposes strict penalties for violations.

Canada and Australia: Have privacy laws that offer legal frameworks for patient data, including rights to access, correction, and means for filing complaints.

These comparative models act as benchmarks for India's developing legal framework, highlighting the need for comprehensive legislation, digital security, and privacy measures that focus on patients.

Medical confidentiality and health information privacy are based on ethical responsibilities and strengthened by legal requirements. Ethical principles like autonomy, beneficence, and fidelity guide professional behaviour, while legal frameworks—including constitutional rights, statutory laws, and global best practices—ensure these principles are actionable and accountable.

The combination of ethical and legal standards creates a solid foundation for protecting patient privacy in a more digital and interconnected healthcare landscape. However, advancements in technology, digital records, and telemedicine introduce new challenges. This underscores the importance of continually updating legal and ethical frameworks to protect health information.

National legal framework

In India, the protection of medical confidentiality and health information privacy comes from a mix of constitutional rights, laws, court decisions, and professional guidelines. Unlike some places that have a single, comprehensive law, India uses several overlapping legal systems to protect patient data. This chapter explores the national legal environment, highlighting important laws, regulatory bodies, and significant court cases that shape the

responsibilities of healthcare providers and the rights of patients.

1. Constitutional Foundations

The right to privacy is recognized as a fundamental right under Article 21 of the Indian Constitution (Justice K.S. Puttaswamy v. Union of India, 2017) ^[1]. This right serves as the main constitutional basis for health information privacy. The Supreme Court ruled that personal data, including medical records, is part of privacy and cannot be shared without consent, except in legally allowed situations.

This constitutional recognition creates a dual responsibility:

- Healthcare providers must safeguard patient information as part of the patient's fundamental rights.
- State authorities must create data protection frameworks and policies to prevent unauthorized access or misuse of medical data.

2. Statutory and Regulatory Framework

Several laws impact confidentiality and privacy in India:

- **Indian Penal Code, 1860 (IPC):**
- **Section 72 (IT Act added):** Penalizes breaches of confidentiality by those who legally hold personal information.
- General principles under IPC apply if disclosing medical records leads to harm, defamation, or criminal liability.
- Indian Evidence Act, 1872 (Sections 126–129):
- Protects confidential communications between doctors and patients.
- Doctors cannot be forced to reveal patient information in court, except under specific legal provisions.
- Information Technology Act, 2000 (IT Act) and Rules:
- Sections 43A and 72A impose penalties for unauthorized access to or disclosure of sensitive personal data, including medical records.
- The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, set standards for how health data should be stored, consented, and shared in digital formats.

Proposed Personal Data Protection Bill, 2019:

Identifies health data as “sensitive personal information” and requires explicit consent, purpose limitation, data localization, and breach notifications.

Though it is still pending, the Bill is part of India's effort toward better digital data protection, aligning with international standards like GDPR.

Consumer Protection Act, 2019

Though it mainly deals with service quality, it indirectly assigns healthcare providers the responsibility to manage patient data properly and keep it confidential.

Professional Regulations

National Medical Commission (NMC) / Medical Council of **India (MCI) Regulations:** Physicians must follow ethical codes to maintain confidentiality unless legally required to disclose information.

Violations can lead to disciplinary action, suspension, or loss of license.

3. Landmark Judicial Decisions

Indian courts have played an important role in clarifying medical confidentiality and privacy:

Retd. Justice K.S Puttaswamy v. Union of India (2017)

Confirmed that privacy is a fundamental right, covering medical data, and emphasized the need for consent before disclosing any information.^[1]

Dr. Suresh Gupta v. Govt. of NCT Delhi (2004)

Acknowledged the significance of confidentiality in medical practice and warned against unnecessary intrusions.^[1]

State of Maharashtra v. Dr. Praful B. Desai (2003)

Addressed issues of patient consent and disclosure related to medical procedures and treatment records.

These decisions reinforce that patient consent and ethical management of information are key to legal duties.^[1]

4. Consent and Disclosure

- Consent is the foundation of confidentiality. Indian law states that patient information can only be disclosed:
 1. With explicit patient consent.
 2. When required by law (such as reporting communicable diseases or court orders).
 3. In the public interest, but only through minimal disclosure and with safeguards.

Guidelines from the NMC and the Ministry of Health stress that any disclosure must be limited, documented, and justified, ensuring minimal invasion of privacy while meeting legal or public health needs.

5. Digital Health and Regulatory Challenges

The growth of electronic health records (EHRs), telemedicine, and cloud storage has brought new regulatory challenges:

- Ensuring secure storage and access controls to stop unauthorized data access.
- Balancing patient privacy with the needs of public health monitoring and research.
- Addressing challenges of cross-border data transfer and integration with international health information standards.
- While provisions in the IT Act offer some protections, the lack of comprehensive national health data laws leaves gaps in enforcement, breach reporting, and standardization

India's legal framework for medical confidentiality and health information privacy is complex, combining constitutional rights, statutory laws, professional ethics, and judicial interpretation. While this framework offers essential protections, challenges remain due to digitalization, fragmented laws, and uneven enforcement.

Proper protection of patient data requires not only following existing laws but also improving regulatory systems, standardizing digital practices, and integrating emerging technologies with privacy protections. The next chapter will explore contemporary challenges, including cybersecurity risks, telemedicine, and ethical issues in the digital healthcare landscape.

Challenges and contemporary issues

The growing digitalization of healthcare, the rise of telemedicine, and the widespread use of electronic health records (EHRs) have dramatically changed how we think about medical confidentiality and health information privacy. While these innovations make healthcare easier to access and more efficient, they also bring new ethical, legal, and technical issues. Finding a balance between patient privacy and the needs of public health, medical research, and data-driven advancements has become a critical issue. This chapter examines the current challenges and systemic problems related to confidentiality and privacy in India.

1. Digitalization of Health Records

Electronic health records (EHRs) store detailed patient data, which includes medical history, test results, prescriptions, and billing information. While EHRs improve efficiency and the continuity of care, they also raise the risk of unauthorized access and data breaches.

Key challenges include:

- **Cybersecurity Threats:** Hacking, phishing, and ransomware attacks can compromise sensitive health information.
- **Inadequate Infrastructure:** Many hospitals lack strong IT systems and trained staff to manage and protect electronic records.
- **Data Misuse:** EHRs can be misused by insurers, employers, or other parties without the patient's consent.

Although the IT Act and proposed Personal Data Protection Bill provide some protections, enforcement is inconsistent, which leaves patients at risk.

2. Telemedicine and Remote Healthcare

The COVID-19 pandemic sped up the use of telemedicine, allowing for remote consultations and treatment. While this is beneficial, telemedicine raises privacy concerns, such as:

- **Transmission Security:** Patient information shared over unsecured networks can be intercepted.
- **Consent Challenges:** Patients may not fully understand how their data will be stored or shared.
- **Platform Accountability:** Third-party applications may keep sensitive health data without proper protections.

These issues highlight the need for clear rules for telehealth services, including encryption standards, consent protocols, and data retention policies.

3. Ethical Dilemmas in Data Sharing

Modern healthcare often requires sharing data for research, public health monitoring, and policy development. Ethical dilemmas arise when balancing individual privacy with collective benefits:

- **Research and Big Data Analytics:** Anonymized patient data can improve healthcare outcomes, but improper de-identification can still expose personal information.
- **Public Health Surveillance:** Reporting infectious diseases or vaccination status may conflict with individual privacy rights.

- **Genetic and Genomic Data:** Advances in genomics raise concerns about consent, discrimination, and family privacy.

Ethical frameworks and legal protections must change to ensure that data sharing respects patient autonomy while providing societal benefits.

4. Breaches of Confidentiality

Medical confidentiality breaches are a significant issue in India, including:

- **Unauthorized Disclosure by Healthcare Professionals:** Sharing patient information with colleagues or the media without consent.
- **Institutional Failures:** Hospitals may not implement adequate safeguards, leading to accidental leaks or access by unauthorized staff.
- **Technological Vulnerabilities:** Cloud storage, mobile applications, and electronic prescribing systems might not be secure enough.

Consequences of breaches can include loss of patient trust, damage to reputation, and potential legal liability under the IPC, IT Act, or civil law.

5. Challenges in Legal Enforcement

Despite protections in the constitution and laws, enforcing medical confidentiality faces several challenges:

Fragmented Legal Framework: Overlapping laws create uncertainty for both patients and healthcare providers.

Limited Awareness: Patients often do not know their privacy rights and legal options.

Judicial and Regulatory Delays: Cases involving health data breaches can be delayed by procedural inefficiencies or lack of expert evaluation.

Absence of Standardization: No uniform national standards exist for electronic health records, telemedicine platforms, or consent documentation.

These gaps lead to inconsistent enforcement and threaten patient data.

6. Emerging Technologies and Privacy Concerns

Technological advancements present both opportunities and risks:

- **Artificial Intelligence (AI) in Healthcare:** AI algorithms depend on large datasets, raising concerns about anonymization, consent, and bias.
- **Blockchain for Health Records:** Although it promises secure data storage, there are implementation challenges and difficulties integrating with current systems.
- **Mobile Health Apps:** Many apps collect sensitive data without proper privacy disclosures or encryption, putting patients at risk.

Balancing innovation with privacy protection requires solid regulatory frameworks, ethical guidelines, and technological safeguards.

7. Balancing Patient Rights and Public Interest

A significant challenge today is reconciling individual privacy with public health and research needs. For instance:

- Reporting infectious diseases may be essential for public health but can conflict with individual consent.
- Sharing anonymized patient data for research can enhance medical knowledge but may risk re-identification.
- Policymakers need to ensure that legal and ethical frameworks set clear boundaries to protect privacy while allowing for necessary healthcare services.

Today's healthcare environment presents complex challenges for medical confidentiality and health information privacy. Digitalization, telemedicine, big data, and AI increase risks, while fragmented laws and limited understanding hinder enforcement. Addressing these issues requires a multifaceted approach, including:

- Legislation that covers digital health and data protection.
- Clear ethical guidelines for consent, data sharing, and disclosure.
- Strong technological safeguards and cybersecurity measures.
- Education for patients and professionals about privacy rights and responsibilities.

Recommendations and future directions

The protection of medical confidentiality and health information privacy is becoming more complex due to digitalization, telemedicine, and the extensive use of data. India has made progress through recognizing privacy in its constitution and introducing some laws, but the current systems are still fragmented and not fully enforced. This chapter provides recommendations aimed at improving legal, ethical, and technological protections, while also addressing the changing needs of today's healthcare.

1. Strengthening Legal Frameworks

Comprehensive Health Data Protection Law:

- India should create a specific law that focuses on medical confidentiality, electronic health records, and digital health platforms.
- The law should define what counts as sensitive health data, what disclosures are allowed, and the penalties for breaches.

Following international guidelines like GDPR and HIPAA would help build trust and support cross-border healthcare cooperation.

Uniform Consent Protocols

- Standardized methods for obtaining, documenting, and withdrawing consent should be used in all healthcare settings.
- Patients must give explicit consent for data sharing, secondary research, and electronic transmission.

Clear Regulatory Guidelines for Telemedicine and Health Apps

- The Ministry of Health, with input from the NMC, should set mandatory regulations for telehealth services, cloud storage, and mobile health apps.
- These guidelines should ensure data encryption, secure storage, and access control.

2. Enhancing Institutional Mechanisms

Specialized Medico-Legal Units

Create specific units in hospitals and state health departments to manage data protection, report breaches, and address patient complaints.

Strengthening Professional Oversight

The NMC and State Medical Councils should take disciplinary action for breaches of confidentiality and maintain clear processes for complaints.

Capacity Building

Train healthcare workers on privacy laws, ethical responsibilities, and cybersecurity practices to help prevent unintentional breaches.

3. Technological Safeguards

Cybersecurity Standards

Use strong encryption, access control, and audit systems for electronic health records.

Promote the use of blockchain and secure cloud storage for sensitive medical data.

Anonymization and De-Identification

For research and data-sharing, patient data should be properly anonymized to prevent re-identification while keeping it usable.

Data Breach Notification Protocols

Hospitals and digital platforms must alert patients and authorities quickly in the event of a breach, allowing for timely corrective actions.

4. Public Awareness and Patient Empowerment

Patient Education Programs

Launch nationwide campaigns to inform patients about their privacy rights, consent processes, and ways to seek help.

Access to Personal Health Data

Patients should have the right to see, correct, and limit sharing of their health information, which promotes transparency and trust.

Research and Policy Development

Ethical Data Use Guidelines

Create clear rules for big data analytics, AI use, and genomic research to balance innovation with privacy.

Periodic Policy Review

Policies and laws need to be regularly updated to keep up with new technologies, digital health developments, and global best practices.

The landscape of medical confidentiality and health information privacy is changing quickly, driven by new technologies and increasing data use in healthcare. Safeguarding patient information requires a multi-faceted approach that combines clear laws, ethical behaviour, technological protections, and public awareness. By putting in place thorough laws, strong institutional systems, and patient-focused policies, India can build a secure, trustworthy, and transparent healthcare environment. These reforms will not only protect patient rights but also encourage innovation, efficiency, and responsibility in

modern medical practice, ensuring that privacy and progress can coexist.

Conclusion

Medical confidentiality and health information privacy are essential parts of ethical and legal healthcare practice. They protect patient autonomy, build trust in the patient-doctor relationship, and ensure responsible handling of sensitive information. Over the years, India's legal and ethical framework has changed significantly. The constitutional recognition of privacy under Article 21, the safeguards in the IT Act, Indian Evidence Act, and Consumer Protection Act, along with the ethical obligations set by the National Medical Commission, create the foundation for protecting patient data. Judicial decisions, such as Justice K.S. Puttaswamy v. Union of India (2017),^[1] have also highlighted the importance of consent, confidentiality, and data protection in today's healthcare.

Despite these improvements, the current healthcare system faces several challenges. Digitalization, telemedicine, electronic health records, mobile health applications, and big data analytics have raised significant risks of unauthorized access, breaches, and misuse. Fragmented laws, limited public awareness, inconsistent enforcement, and weak institutional frameworks worsen these vulnerabilities. Ethical dilemmas arise when trying to balance individual privacy with public health needs, research demands, and technological progress.

To tackle these challenges, a broad approach is necessary. Strong legislation, clear consent processes, effective cybersecurity measures, specialized medico-legal teams, and regular policy updates can help create a solid framework. Educating and empowering patients is equally important so they understand their rights and how to protect their data. Ethical guidelines for research, AI use, and telehealth services should support legal measures to preserve public trust and professional responsibility.

In conclusion, the shifting landscape of medical confidentiality and health information privacy requires ongoing updates to laws, ethical standards, and technological protections. By combining legal clarity, ethical duty, technological progress, and public awareness, India can build a healthcare system that respects patient privacy, encourages trust, and supports safe, effective, and innovative medical practices. The objective is not just to avoid breaches but to create a lasting culture of confidentiality that strengthens both patient rights and the integrity of the healthcare system.

References

1. K.S. Puttaswamy (Retd) vs Union of India, 2017:10:1.
2. Mr. 'X' vs Hospital 'Z', AIR 1999 SC 495.
3. Ministry of Health and Family Welfare, Government of India. Draft Digital Information Security in Healthcare Act (DISHA), 2019.
4. Ministry of Electronics and Information Technology, Government of India. Digital Personal Data Protection Act, 2023.
5. Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.
6. Centre for Internet and Society. Health Data in India: A Regulatory Landscape, 2019.
7. Mishra, N. Privacy and the Right to Information Act, 2005. Indian Journal of Medical Ethics, 2017.
8. Kaushik, M. Privacy and Confidentiality of Health Records: A Legal Perspective. Journal of Indian Law Institute, 2020.