INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DATA PRIVACY IN BIO MEDICAL RESEARCH AN ANALYSIS

AUTHORED BY – ADV. AKHILA LEKSHMI VL
Central University of Kerala

INTRODUCTION

The importance of privacy was acknowledged as far back as the time of the Hippocratic Oath[1].Both consequentialist and deontological ethical justifications exist for protecting privacy in the patient–provider relationship[2]. This is essential, given the fiduciary nature of the doctor-patient relationship and the mutual expectations of trust between patient and doctor. Privacy in healthcare has many facets, including informational privacy, physical privacy, associational privacy, proprietary privacy and decisional privacy[3]

Biomedical research stands at the forefront of scientific advancement, driving innovations that enhance human health and well-being. In the era of data-driven biomedical research, the protection of sensitive information has become a matter of utmost importance. With vast amounts of personal health data, genetic profiles, and clinical records being collected and analysed, ensuring the security and confidentiality of this data is critical not only for compliance with regulations but also for upholding the trust of patients and the integrity of research outcomes. Ensuring the confidentiality, integrity, and appropriate use of biomedical data is paramount not only for safeguarding individual rights but also for maintaining public trust in scientific endeavours.

THE SIGNIFICANCE OF DATA SECURITY IN BIOMEDICAL RESEARCH

The significance of data security in the realm of biomedical research cannot be overstated. In an era where data fuels scientific discovery, informs medical treatments, and shapes public

[1] Arenas A, translator. Hippocrates' Oath. Boston University website. Cited 2023 Oct 10. Available from: https://www.bu.edu/arion/files/2010/03/Arenas_05Feb2010_Layout-3.pdf
[2] Jain D. Regulation of Digital Healthcare in India: Ethical and Legal Challenges. Healthcare (Basel). 2023 Mar 21; 11(6):911. https://doi.org/10.3390%2Fhealthcare11060911
[3] Mani T. Privacy in Healthcare: Policy Guide. Centre for Internet and Society. Centre for Internet and Society website. 2014 Aug 26[Cited 2023 Oct 10]. Available from: https://editors.cis-india.org/internet-governance/blog/privacy-healthcare.pdf

ISSN: 2582-6433

health policies, safeguarding the integrity and confidentiality of this data is paramount.

- **Protecting Patient Privacy:** Biomedical research often involves the collection and analysis of highly sensitive information, including individuals' medical histories, genetic profiles, and personal health data. This wealth of personal information is entrusted to researchers by patients and participants with the expectation that their privacy will be respected and their data handled with the utmost care. Any breach of data security not only violates this trust but also poses a threat to individuals' privacy rights.[4]
- **Ensuring Research Integrity:** The integrity of biomedical research hinges on the accuracy and reliability of data. Researchers rely on data to make groundbreaking discoveries, identify disease trends, and develop new treatments. Any compromise in data security can lead to data manipulation or corruption, casting doubt on the legitimacy of research findings. Ensuring data security is, therefore, fundamental to upholding the credibility and trustworthiness of research outcomes.
- **Legal and Ethical Obligations:** Beyond ethical considerations, biomedical research is subject to a web of regulations and laws governing data protection. For instance, the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe mandate strict data security measures for healthcare and research institutions. Non-compliance with these regulations not only carries legal consequences but also undermines the ethical foundations of research.
- **Trust and Participation:** Trust is the bedrock of biomedical research. Patients and research participants willingly contribute their data and personal information to advance scientific knowledge and improve healthcare outcomes. Any data breach or security lapse erodes this trust, making individuals hesitant to participate in research studies. A loss of trust can hinder data collection efforts, impede scientific progress, and limit the pool of willing participants.
- **Public Perception:** The impact of data security breaches in biomedical research extends beyond individual studies. High-profile incidents can damage the public's perception of the entire research enterprise. Such incidents can lead to scepticism about data handling practices, research ethics, and the safety of medical treatments. Rebuilding public trust can be a lengthy and arduous process.

[4] Cohen IG, Lynch HF, Vayena E, Gasser U. Big data, health law, and bioethics: Cambridge University Press; 2018

ISSN: 2582-6433

CHALLENGES IN DATA SECURITY

Biomedical research operates within a complex and dynamic landscape, and this complexity extends to the domain of data security. While the need to protect sensitive biomedical data is indisputable, researchers and institutions face a series of unique challenges in achieving robust data security.

- **Diverse Data Sources:** Biomedical research draws data from a wide array of sources, including electronic health records (EHRs), clinical trials, genetic databases, wearable devices, and patient surveys. This diversity presents a formidable challenge in terms of data integration and security. Each data source may have distinct formats, storage mechanisms, and security protocols, making it difficult to establish a unified security framework.[5]
- **Privacy Concerns:** The nature of biomedical data often involves highly sensitive and personal information. This includes medical histories, genetic profiles, disease diagnoses, and treatment outcomes. Researchers must navigate a delicate balance between accessing this valuable information for scientific purposes and safeguarding individuals' privacy rights. Privacy concerns can intensify when data is shared across institutions, regions, or countries, necessitating rigorous privacy protection measures.[6]
- **Data Sharing and Collaboration:** Biomedical research frequently relies on collaboration among researchers, institutions, and healthcare providers. Sharing data is essential for advancing scientific knowledge and accelerating medical breakthroughs. However, data sharing introduces inherent security challenges. Balancing data accessibility with stringent security measures can be challenging, especially when multiple parties with varying levels of security infrastructure are involved.
- **Data Volume and Complexity:** The sheer volume of biomedical data generated today is staggering. Large-scale genomics projects, clinical trials, and electronic health records contribute to the exponential growth of data. Managing, securing, and analysing such vast datasets is a technical challenge. Additionally, the complexity of biomedical data, which often includes structured and unstructured information, further complicates security efforts.
- **Data Lifecycle Management:** The lifecycle of biomedical data, from collection to disposal, demands meticulous management. Each phase of the data lifecycle presents

[5] Jain P, Gyanchandani M, Khare N. Differential privacy: its technological prescriptive using big data. Journal of Big Data 2018; 5:1–24
[6] Price WN 2nd, Cohen IG. Privacy in the age of medical big data. Nat Med 2019

ISSN: 2582-6433

unique security considerations. For instance, data must be securely transmitted during collection, protected against unauthorized access during storage, and properly de-identified or anonymized when shared or archived. Managing these aspects cohesively and consistently is a formidable task.

- **Human Error and Insider Threats:** While technology plays a pivotal role in data security, human factors cannot be ignored. Accidental data breaches, misconfigurations, and insider threats pose significant risks. Researchers, healthcare professionals, and staff members may unintentionally mishandle data or fall victim to phishing attacks, emphasizing the need for ongoing education and training in data security best practices.

The challenges in data security within the realm of biomedical research are multifaceted. Researchers and institutions must contend with diverse data sources, navigate privacy concerns, facilitate data sharing, handle vast and complex datasets, manage the data lifecycle, and address human factors. Effectively addressing these challenges requires a comprehensive and adaptive approach to data security, one that acknowledges the unique intricacies of biomedical research while upholding the ethical and legal obligations associated with safeguarding sensitive data.

STRATEGIES FOR ENHANCING DATA SECURITY

Ensuring the security of sensitive biomedical data demands a multifaceted approach that combines technology, policies, and education. Researchers and institutions involved in biomedical research can adopt several strategies to bolster data security effectively.

- **Encryption:** Implementing robust encryption protocols is a fundamental measure to protect data at rest and during transmission. Data encryption transforms information into a format that is unreadable without the corresponding decryption key. This ensures that even if unauthorized access occurs, the data remains secure and unintelligible.
- **Access Controls:** Enforcing strict access controls is critical. Access to sensitive data should be granted only to authorized personnel based on their roles and responsibilities. Role-based access control (RBAC) systems ensure that individuals can access only the data necessary for their specific tasks. Implementing multi-factor authentication (MFA) adds an extra layer of security, requiring multiple forms of verification before granting access.
- **Data Anonymization:** Whenever possible, de-identifying data by removing personally identifiable information (PII) is a powerful security measure. Anonymization

ISSN: 2582-6433

techniques can help protect the privacy of individuals while still allowing for valuable data analysis. Researchers should be cautious about retaining only essential information needed for the research, minimizing the risk associated with data breaches.

- **Regular Auditing and Monitoring:** Continuous monitoring and auditing of data access and usage are essential components of a robust data security strategy. These activities involve tracking who accesses data, when, and for what purpose. Suspicious activities can trigger alerts and investigations, allowing for prompt responses to potential security threats.
- **Employee Training:** Human factors play a significant role in data security. Researchers and staff should receive regular training on data security protocols and best practices. Education programs can raise awareness about the importance of data security and the potential consequences of lapses. Training should encompass topics such as password management, phishing awareness, and secure data handling.[7]

These strategies should be tailored to the specific context of biomedical research, where the protection of sensitive patient information is paramount. Additionally, compliance with relevant regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the General Data Protection Regulation (GDPR) in Europe, is crucial. These regulations provide specific guidelines and requirements for data security in healthcare and research settings.

By adopting these strategies, biomedical researchers and institutions can significantly enhance data security. The implementation of encryption, access controls, data anonymization, regular auditing, and employee training collectively contributes to a robust data security ecosystem. This, in turn, not only safeguards sensitive data but also upholds the ethical and legal obligations associated with biomedical research and healthcare.

LEGAL FRAMEWORKS GOVERNING DATA PRIVACY

Data privacy in biomedical research is governed by a tapestry of international and national laws and regulations. These frameworks establish the standards and obligations for data protection, aiming to harmonize practices and provide legal recourse in case of violations.

[7] Data Privacy in Healthcare Industry: Indian Perspective (By Prof. Prathamesh Churi), https://engineering.nmims.edu/docs/Privacy%20Article.pdf

ISSN: 2582-6433

INTERNATIONAL LEGAL FRAMEWORKS

- **General Data Protection Regulation (GDPR)[8]**

The GDPR, enacted by the European Union (EU) in May 2018, is one of the most comprehensive data protection laws globally. It sets stringent requirements for data processing, emphasizing the protection of personal data and the rights of individuals. Key aspects relevant to biomedical research include:

- **Lawful Basis for Processing**: Researchers must identify a valid legal basis for processing personal data, such as consent, legitimate interest, or public interest.
- **Data Minimization and Purpose Limitation**: Only data necessary for specific research purposes should be collected and processed.
- **Data Subject Rights**: Individuals have rights to access, rectify, erase, and restrict the processing of their data.
- **Data Protection Impact Assessments (DPIAs)**: Required for high-risk data processing activities, including certain biomedical research projects.
- **International Data Transfers**: Strict rules govern the transfer of personal data outside the EU, ensuring that adequate protection is maintained.

The GDPR has extraterritorial reach, meaning it applies to organizations outside the EU that process data of EU residents, significantly impacting global biomedical research practices.

- **Health Insurance Portability and Accountability Act (HIPAA)[9]**

In the United States, HIPAA governs the privacy and security of individuals' health information. Enacted in 1996, HIPAA comprises several rules, with the Privacy Rule and Security Rule being most pertinent to biomedical research.

- **Privacy Rule**: Establishes standards for the protection of individually identifiable health information, known as Protected Health Information (PHI). It restricts the use and disclosure of PHI without patient authorization, except under specific circumstances.
- **Security Rule**: Sets requirements for safeguarding electronic PHI through administrative, physical, and technical safeguards.

[8] Regulation GDP. General data protection regulation (GDPR)–official legal text. Gen Data Prot Regul (2016)
[9] United States. Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. US Statut Large 1996; 110:1936–2103.

ISSN: 2582-6433

- **Research Exceptions**: HIPAA allows for the use of PHI in research under certain conditions, such as obtaining authorization from participants or obtaining a waiver from an Institutional Review Board (IRB).

HIPAA compliance is critical for biomedical researchers in the U.S., ensuring that health data is handled responsibly and ethically.

➢ **Other International Laws and Guidelines**

Beyond GDPR and HIPAA, various other international instruments influence data privacy in biomedical research:

- **The Declaration of Helsinki**: A set of ethical principles for medical research involving human subjects, emphasizing informed consent and confidentiality.
- **The International Covenant on Civil and Political Rights (ICCPR)**: Article 17 protects against arbitrary or unlawful interference with privacy.
- **OECD Guidelines on Privacy and Transborder Flows of Personal Data**: Provide a framework for protecting privacy in international data transfers.
- **Asia-Pacific Economic Cooperation (APEC) Privacy Framework**: Offers guidelines for data privacy protection and cross-border data flows among APEC member economies.

INDIAN LEGAL FRAMEWORKS

India has been progressively developing its data protection laws, influenced by international standards yet tailored to its unique socio-economic context.

- **Information Technology Act, 2000 and Amendments**

The IT Act, 2000, along with subsequent amendments, serves as the primary legislation governing electronic data in India. Key provisions related to data privacy include:

- **Section 43A**: Mandates compensation for failure to protect sensitive personal data by body corporates.
- **Section 72A**: Penalizes disclosure of information in breach of confidentiality.
- **Rules under the IT Act**: Including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which define sensitive personal data and prescribe measures for its protection.

While the IT Act provides a foundation for data protection, it has been criticized for being insufficiently comprehensive in addressing modern data privacy challenges, particularly in the biomedical research context.

ISSN: 2582-6433

- **the Sensitive Personal Data or Information (SPDI) Rules, 2011** which were notified under IT act.
- **the Digital Personal Data Protection Act 2023 (DPDP 2023)**.

in addition, health-specific data protection frameworks have been proposed in India, including the **Digital Information Security in Healthcare Act (DISHA) and the Health Data Management Policy, 2022 (HDMP).**[10]

DISHA is an act to provide for establishment of national and state health authorities and health information exchange; to standardize and regulate the processes related to collection, storing, transmission, and use of digital health data; and ensure reliability, data privacy, confidentiality, and security of digital health data and such other matters related and incidental thereto.
With the enactment of the DPDP Act 2023, in India, Section 43A of the IT Act, and the SPDI Rules, passed under Section 43A, have been replaced. The proposed health-specific data protection frameworks, including the HDMP and DISHA, are sector-specific frameworks that have not been made redundant by the recent general legislation, DPDP 2023.

But there are **several drawbacks in the DPDP 2023** like:

- does not define sensitive personal data;
- allows data processing without *explicit consent* — which has a higher threshold than regular consent;
- does not provide to the data principal the rights to ownership, to restrict or object to use of data, to data portability, or to seek compensation;
- does not mandate the use of health data only in the data principal's best interest and for direct care, or restrict the processing of health data for commercial purposes, or ensure a privacy by design policy;
- does not require a Data Protection Impact Assessment for all data fiduciaries processing health data.

Analysis of the Digital Personal Data Protection Act, 2023

As per DPDP 2023, the enacted data protection legislation in India, personal data can be processed only with consent or for certain legitimate uses (Section 4). An individual's consent "shall be free, specific, informed, unconditional and unambiguous with a clear affirmative

[10] Sharma RS, Rohatgi A, Jain S, Singh D. The Ayushman Bharat Digital Mission (ABDM): making of India's Digital Health Story. CSIT 2023; 11:3–9.

ISSN: 2582-6433

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." (Section 6).

When consent is sought, information must also be provided containing the description of personal data and the purpose of processing it (Section 5). Section 7 specifies that data can be processed for "certain legitimate uses" on the condition that the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and "has not indicated to the Data Fiduciary that she does not consent to its use". Other conditions for certain legitimate use of data include "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" and "to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health." (Section 7).[11]

The DPDP 2023 has reduced the level of protection for health data compared to the DPB 2021.

- Unlike the DPB 2021, the DPDP 2023 does not define health data and does not categorise data as sensitive personal data.
- Unlike the DPB 2021 which required explicit consent that cannot be inferred from conduct in context, the DPDP allows data processing when data is voluntarily provided. This raises several concerns. Will the data principal be aware of the scope of the processing? If adequate safeguards are not provided, can "certain legitimate uses" be abused for secondary processing of data, affecting the data principal's privacy? The privacy of individuals can be affected when the scope of processing is not clearly defined and there is no limitation of purpose. It could lead to the processing of health data for various secondary purposes, such as commercial purposes, which go beyond merely providing health services. When the health data is misused for unspecified purposes, it could lead to harms such as discriminatory treatment of data principals, breach of privacy, and loss of control of health-related data.
- The DPDP 2023 lowers the level of protection provided in DPB 2021 in another way. Section 10 of the DPDP 2023 defines significant data fiduciaries and requires them to undertake data protection impact assessment. A data protection impact assessment

[11] Digital Personal Data Protection act 2023: Ministry of Electronics and Information Technology, Government of India (no date) Digital Personal Data Protection Act 2023 | Ministry of Electronics and Information Technology, Government of India. Available at: https://www.meity.gov.in/content/digital-personal-data-protection-act-2023

ISSN: 2582-6433

requires describing "the rights of Data Principals and the purpose of processing of their personal data, [and] assessment and management of the risk to the rights of the Data Principals" (Section 10, DPDP 2023). Such an assessment was mandatory for processing *sensitive personal data*, under the DPB 2021. The DPB required significant data fiduciaries to carry out a data protection impact assessment when they intend to undertake processing involving the use of *sensitive personal data* (Clause 27). On the other hand, the DPDP 2023 lowers the level of protection, as it does not define sensitive personal data and *therefore*, does not mandate that significant data fiduciaries need to undertake data protection impact assessment for processing *sensitive personal data.*

The HDMP and the Digital Personal Data Protection Act, 2023

The level of protection under the draft HDMP (the Health Data Management Policy, 2022) is greater than under the DPDP. While the HDMP makes explicit consent necessary for processing personal data, the DPDP allows data processing on the ground of certain legitimate uses when the data is voluntarily provided. The HDMP provides rights to the data principal that are missing in the DPDP 2023. For instance, the HDMP provides the right to restrict or object to disclosure of personal data by the data fiduciary, and the right to data portability which makes the data available to the data principal in a commonly used format, which can be shared easily (Clause 14). While the HDMP requires provision of a privacy by design policy, the DPDP 2023 does not recognise the principle of privacy by design. However, the DPDP provides for a higher maximum penalty than the HDMP. Moreover, while matters go to the Data Protection Board of India under the DPDP, grievance redressal under the HDMP involves approaching the data protection officer of the data fiduciary followed by the Ayushman Bharat Digital Mission grievance redress officer ABDM-GRO (Clause 32).

The question is: when the HDMP and DPDP provide for different standards of protection, which would take precedence? Would the HDMP prevail as it is specific to the health sector, or would the DPDP prevail as it is a legislation and not a policy like the HDMP?

Other Relevant Indian Laws and Guidelines

- **The Clinical Establishments (Registration and Regulation) Act, 2010**: Regulates clinical establishments, which may involve handling patient data.
- **Digital information security in healthcare act (DISHA)**
- **Health data management policy 2022**

ISSN: 2582-6433

- **National Health Policy, 2017**: Emphasizes the importance of protecting health information as part of broader health system strengthening.
- **Ethical Guidelines by the Indian Council of Medical Research (ICMR)**: Provide specific guidance on handling personal data in biomedical research, emphasizing confidentiality and informed consent.

LANDMARK JUDGMENTS ON DATA PRIVACY IN BIOMEDICAL RESEARCH

Judicial decisions have played a pivotal role in shaping data privacy standards, interpreting legal provisions, and setting precedents that influence biomedical research practices.

INTERNATIONAL LANDMARK JUDGMENTS

- **European Union: Schrems II (Data Privacy and International Transfers)[12]**

In July 2020, the Court of Justice of the European Union (CJEU) delivered the Schrems II decision, invalidating the EU-US Privacy Shield framework for transatlantic data transfers. This judgment underscored the necessity for adequate data protection standards and influenced how biomedical research entities handle international data flows, particularly when collaborating across borders. Researchers must now rely on mechanisms like Standard Contractual Clauses (SCCs) and ensure that data transfers meet GDPR's stringent requirements.

- **United States: HIPAA Enforcement Cases**

Several notable cases have shaped HIPAA's application:

- **HIPAA Violation Cases**: The Office for Civil Rights (OCR) has fined numerous entities for failing to comply with HIPAA's privacy and security rules. For example, the Anthem Inc. case in 2018 resulted in a $16 million settlement for a massive data breach involving 79 million individuals' PHI.
- **Document v. Texas (2022)[13]**: While not directly a HIPAA case, it addressed privacy concerns over law enforcement access to medical records, reflecting the broader implications of data privacy in sensitive contexts.

These enforcement actions highlight the importance of stringent compliance and the severe consequences of negligence in data protection.

[12] Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18) https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf
[13] UNITED STATES ET AL. v. TEXAS ET AL https://www.supremecourt.gov/opinions/22pdf/22-58_i425.pdf

ISSN: 2582-6433

INDIAN LANDMARK JUDGMENTS

- The issue of privacy in healthcare came up in India in the 1998 case of ***Mr X v Hospital Z***.[14] Mr X was found to be HIV+ when he donated blood. The allegedly unauthorised disclosure of his HIV+ status by the hospital resulted in Mr X's marriage being called off, leading him to seek legal redress. The Court held that doctors must maintain secrecy about their patients. However, the Court also held that "public interest would override the duty of confidentiality, particularly where there is an immediate or future health risk to others" — in this case the risk to the health of the woman who was to marry the appellant.
- In another case, the Supreme Court of India stated that a hospital's unauthorised disclosure of medical records is an invasion of privacy. Furthermore, that when such data are required for legitimate purposes such as analysis of an epidemic, the anonymity of individuals must be
- **The Puttaswamy Judgment (Right to Privacy as a Fundamental Right)**
  In August 2017, the Supreme Court of India delivered a landmark judgment in the case of *Justice K.S. Puttaswamy (Retd.) vs. Union of India*,[15] declaring the Right to Privacy as a fundamental right under the Indian Constitution (Article 21). This judgment has profound implications for data privacy in all sectors, including biomedical research. It established that any data processing activities must respect the intrinsic right to privacy, mandating that:
  - **Consent is Informed and Voluntary**: Participants must be fully aware of how their data will be used.
  - **Data Minimization and Purpose Limitation**: Data collection should be limited to what is necessary for the research purpose.
  - **Protection Against Unauthorized Access**: Robust security measures must be in place to prevent data breaches.

The Puttaswamy judgment has been instrumental in pushing for more comprehensive data protection laws, such as the Personal Data Protection Bill.

[14] Supreme Court of India. Mr X v Hospital Z. Appeal (Civil) 4641 of 1998. 1998 Sep 1[Cited 2023 Oct 10]. Available from: https://indiankanoon.org/doc/382721/
[15] Supreme Court of India. Justice K.S. Puttaswami and another Vs. Union of India. Writ Petition (Civil) 494 of 2012. 2018 Sep 26[Cited 2023 Oct 10]. Available from: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

ISSN: 2582-6433

ETHICAL CONSIDERATIONS IN DATA PRIVACY FOR BIOMEDICAL RESEARCH

Beyond legal compliance, ethical considerations are paramount in handling biomedical data. These include:

Balancing Research Advancement and Privacy Protection

Biomedical research seeks to advance knowledge and improve health outcomes, often relying on large datasets that can lead to significant societal benefits. However, this must be balanced against the need to protect individual privacy. Ethical research requires ensuring that the pursuit of knowledge does not infringe on personal rights or lead to harm.

Informed Consent and Transparency

Obtaining informed consent is fundamental. Participants must understand what data is being collected, how it will be used, who will have access, and the potential risks involved. Transparency in data handling practices builds trust and upholds ethical standards.

Data Anonymization and Security Measures

Anonymizing data reduces privacy risks by removing personally identifiable information. However, as data analytics become more sophisticated, the risk of re-identification increases. Implementing robust security measures, such as encryption and access controls, is essential to protect data integrity and confidentiality.

Ethical Oversight and Governance

Institutional Review Boards (IRBs) or Ethics Committees play a critical role in overseeing research projects, ensuring that data privacy measures are adequately addressed. Establishing clear governance frameworks helps maintain ethical standards and accountability.

CONCLUSION

Data privacy in biomedical research is a critical issue that intertwines legal, ethical, and practical dimensions. As biomedical research continues to evolve, the protection of personal data remains paramount to safeguarding individual rights and maintaining public trust. Legal frameworks, both international and Indian, provide the foundational structures necessary for data protection, while landmark judgments further define and enforce these protections. Ethical

ISSN: 2582-6433

considerations and future-oriented strategies are essential to navigate the complexities of data privacy in an increasingly data-driven world. By fostering robust legal compliance, ethical research practices, and technological innovation, the biomedical research community can achieve its goals without compromising the privacy and dignity of individuals. In an age were data drives biomedical breakthroughs, the security of that data cannot be overlooked. The consequences of data breaches extend far beyond legal penalties, affecting patients' trust and the credibility of research outcomes. By implementing robust security measures, biomedical researchers can uphold the integrity of their work and protect the sensitive information entrusted to them.

REFERENCES

1. Arenas A, translator. Hippocrates' Oath. Boston University website. Cited 2023 Oct 10. Available from: https://www.bu.edu/arion/files/2010/03/Arenas_05Feb2010_Layout-3.pdf
2. Jain D. Regulation of Digital Healthcare in India: Ethical and Legal Challenges. Healthcare (Basel). 2023 Mar 21; 11(6):911. https://doi.org/10.3390%2Fhealthcare11060911
3. Mani T. Privacy in Healthcare: Policy Guide. Centre for Internet and Society. Centre for Internet and Society website. 2014 Aug 26[Cited 2023 Oct 10]. Available from: https://editors.cis-india.org/internet-governance/blog/privacy-healthcare.pdf
4. Cohen IG, Lynch HF, Vayena E, Gasser U. Big data, health law, and bioethics: Cambridge University Press; 2018
5. Digital Personal Data Protection act 2023: Ministry of Electronics and Information Technology, Government of India (no date) Digital Personal Data Protection Act 2023 | Ministry of Electronics and Information Technology, Government of India. Available at: https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
6. Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18)
7. https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf
8. [1] UNITED STATES ET AL. v. TEXAS ET AL
9. https://www.supremecourt.gov/opinions/22pdf/22-58_i425.pdf
10. Supreme Court of India. Mr X v Hospital Z. Appeal (Civil) 4641 of 1998. 1998 Sep 1[Cited 2023 Oct 10]. Available from: https://indiankanoon.org/doc/382721/

ISSN: 2582-6433

11. Supreme Court of India. Justice K.S. Puttaswami and another Vs. Union of India. Writ Petition (Civil) 494 of 2012. 2018 Sep 26[Cited 2023 Oct 10]. Available from: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
12. Koenderman J. Discrimination and privacy concerns at the intersection of healthcare and big data. Cardozo Law Rev. 2020
13. Ministry of Law and Justice, Govt of India. The Information Technology Act 2000. Act No. 21 0f 2000. 2000 Oct 17[Cited 2023 Oct 10]. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf