SECONDARY USE OF MEDICAL DATA FOR RESEARCH AND AI: REGULATORY CONFLICTS AND HARMONIZATION ACROSS GDPR, HIPAA, AND DPDP ACT

Sanskriti Jakhmola, Law Student, Law College Dehradun, Uttaranchal University, Dehradun[1]

Asst. Prof. Nikunj Yadav, Asst. Prof., Law College Dehradun, Uttaranchal University, Dehradun[2]

ABSTRACT

Secondary use of medical data, i.e., the use of health information for purposes other than direct patient care, has become the mainstay of biomedical research, artificial intelligence (AI), and public health analytics. This rapid deployment of health data, however, raises intricate regulatory challenges, especially when differing legal regimes are involved.

By comparing the European Union's General Data Protection Regulation (GDPR), the United States' Health Insurance Portability and Accountability Act (HIPAA), and India's Digital Personal Data Protection (DPDP) Act, this article examines how each framework controls the use of secondary data for research and AI development. The study identifies significant divergence areas, among others, requirements for consent, research bases allowed, standards for anonymization and de, identification, as well as limitations on data transfers across borders.

While GDPR implements a rights, based model with tight safeguards and strictly defined research exceptions, HIPAA offers a greater degree of operational flexibility through its Safe Harbor and limited data set provisions. The DPDP Act, on the other hand, is a consent, focused but still development regime, which, therefore, lacks clarity about research exemptions and government access. The article claims that the splitting of regulations acts as a barrier to the collaboration of health data worldwide, makes the training of AI models more difficult, and puts the risk of re, identification at a higher level. It ends with a proposal of harmonization strategies, such as interoperable anonymization standards, dynamic consent mechanisms, stronger accountability norms, and international cooperation frameworks to facilitate innovation while ensuring patient privacy.

[1] Law Student, Law college Dehradun, Uttaranchal University, Dehradun
[2] Asst. Prof., Law college Dehradun, Uttaranchal University, Dehradun

Introduction: Rise of Secondary Use of Medical Data in Research & AI

These 20 years have been a period of change unseen before in the worldwide healthcare system, which is mainly attributed to the rapid digitalization, the proliferation of electronic health records (EHRs), and the adoption of data, driven technologies in clinical, administrative, and research settings. Within this changing environment, the secondary use of medical data, i.e., the use of personal health information for non, direct patient care purposes, has become one of the major motors of innovation. Secondary uses encompass epidemiological research, public health surveillance, clinical trials, health, system optimization, biomedical research, and, to a great extent, the development and training of artificial intelligence (AI) models in diagnostics, personalized medicine, and drug discovery. The ability to repurpose huge datasets has, thus, become the core of modern healthcare with enormous potential for societal good, at the same time, however, it raises complicated legal, ethical, and regulatory issues.

The increasing application of AI and machine learning (ML) techniques in healthcare is the main factor that significantly amenities the importance of secondary use. In order to find patterns, to make predictions, and generally to enhance clinical decision, making, AI systems require large, diverse, and high, quality datasets. The effectiveness of algorithms employed in cancer detection, predictive risk modeling, population health analytics, and genomics, based precision medicine, for instance, depends solely on the quality of the medical data that they are exposed to. As such, hospitals, research institutes, health, tech companies, and governments are more than ever eager to pool and investigate patient data on a scale that has never been done before. However, this unrelenting pursuit of data, driven innovation is in conflict with a number of long, established privacy principles such as informed consent, purpose limitation, data minimization, and protection of sensitive health information.

Different regulatory systems worldwide have taken various approaches in terms of governing the collection, processing, and secondary use of medical data, hence resultant fragmentation and uncertainty are the major consequences of their lack of unity. The General Data Protection Regulation (GDPR) of the European Union adopts a rights, based, individual, centric perspective and considers health data to be a special category of sensitive data, thereby, it restricts its use in a very stringent manner except in certain cases, e.g., explicit consent, scientific research exemptions, or substantial public interest. Instead of one integrating privacy framework, the United States manages health data mainly through the Health Insurance

Portability and Accountability Act (HIPAA), which is a sectoral law that distinguishes between covered entities (e.g. hospitals, insurers) and business associates, thus allowing secondary use mainly through de, identified datasets under the Safe Harbor and Expert Determination standards. The freshly introduced Digital Personal Data Protection Act, 2023 (DPDP Act) of India is yet another example of a regulatory regime, a consent, driven but adaptable one, in which medical data is categorized as "personal data" in the broadest sense, with certain duties for data fiduciaries and some exemptions for research and government activities.

Even though the global community is progressively more dependent on the secondary use of medical data, the three frameworks studied here still differ significantly in terms of their definitions, standards, and safeguards. As an example, pseudonymization in GDPR still considers data as personal data if re, identification is possible, while HIPAA's Safe Harbor method allows datasets to be used freely once specified identifiers are removed. The DPDP Act of India is yet to set out standards for anonymization with equal rigor and therefore it leaves considerable room for interpretation in terms of medical datasets being utilized for AI development or academic research. Furthermore, cross, border data transfers being a crucial factor for multinational clinical trials and global AI research are at odds with each other: GDPR lays down strict adequacy and safeguard requirements, HIPAA allows transfers under business associate agreements, and the DPDP Act foresees limitations via future government notifications. Such divergences cause operational difficulties for global health, tech companies and prompt them questions regarding compliance, interoperability, and patient trust.

The ethical dimension of the issue makes the situation with secondary use even more complicated. The majority of patients are not aware of how their medical data is reused, let alone that it could be used for commercial AI development. The established model of “specific informed consent” is turned increasingly less feasible with data potentially being reused for unforeseeable future research. The possibility of re, identification from supposedly anonymized datasets, the bias put into AI models, and the unequal distribution of the gains from data, driven research are among the reasons why the public shows distrust towards the whole issue. In response to this, regulators all over the world are feeling the pressure of being required to find a fine balance between enabling data, driven innovation on the one hand and protecting patient privacy and autonomy on the other.

Such a situation highlights the need of a comparative analysis of GDPR, HIPAA, and the DPDP

Act. These three frameworks represent different sets of cultural, legal, and policy values respectively, but at the core they face the same problem, how to make possible a beneficial secondary use of medical data while at the same time ensuring strong safeguards against misuse, discrimination, and breaches. Knowing their differences is important not only for legal scholarship but also for the formation of future regulatory harmonization when healthcare, technology, and global data flows become more and more interlinked.

Regulatory Treatment of Secondary Use of Medical Data

The secondary use of medical data, meaning the use of health information for non, care, related purposes, like research, public health analytics, AI model development, and policy, making, has become an essential topic of debate in data protection laws worldwide. The General Data Protection Regulation (GDPR), the U.S. Health Insurance Portability and Accountability Act (HIPAA), and India's Digital Personal Data Protection Act, 2023 (DPDP Act), are all different in their approach to this question, which is in line with their different legal traditions, policy priorities, and socio, technological contexts. By comparing these regulatory frameworks, one can see that they have similarities but also significant regulatory tensions that determine the legal processing capacity of healthcare institutions, researchers, and AI developers.

GDPR: A Rights, Based Framework with Structured Research Exemptions

The three regimes analyzed, the GDPR being the strictest and most thorough one, is based on the EU's fundamental rights approach to privacy. Medical data is considered one of the "special categories of personal data" (Art. 9), that has very stringent protection. However, the secondary use of data for scientific or historical research is identified as a legitimate societal interest by the GDPR, which allows such data processing in compliance with certain requirements.

The lawful bases most relevant to research include:

- **Explicit consent (Art. 9(2)(a))**, which must be specific, informed, and freely given.

- **Processing necessary for scientific research (Art. 9(2)(j))**, provided that appropriate safeguards such as pseudonymisation, data minimisation, and technical controls are in place.

Under the GDPR, a Data Protection Impact Assessment (DPIA) must be conducted when data processing is considered high risk, and places severe obligations on data controllers for transparency, purpose limitation, and storage limitation. Nevertheless, it provides some leeway for research by allowing for purpose compatibility assessments, thus enabling the secondary use of data without a new consent if the purpose is compatible with the original one. Moreover, supervisory authorities as well as ethics committees have a significant role in facilitating or giving directions for the use of research data, particularly in the case of biobanks and AI training datasets.

Research, related cross, border transfer will only be allowed if there are adequate safeguards, thus posing a challenge for compliance of global health research networks.

HIPAA: A Sector-Specific, Compliance-Oriented Model

A Sector, Specific, Compliance, Oriented Model The HIPAA Privacy Rule takes a very different stance. It is limited to "covered entities" (e.g. hospitals, insurers) and their "business associates", and does not extend to processors of personal data generally. Instead of a rights, based model, HIPAA is mainly compliance, driven and depends on regulated categories of data.

When it comes to the secondary use of data, HIPAA concentrates on the identification of the data. According to HIPAA, de, identified data is no longer "protected health information" (PHI) and accordingly, it can be utilised for research, AI development, and analytics without any limitations.

HIPAA defines two methods for de, identification:

1. Safe Harbor Method – removal of 18 specific identifiers.

2. Expert Determination Method – statistical certification that the risk of re-identification is very low.

For identifiable data, HIPAA allows secondary use only with:

- Individual authorization, which is similar to consent;
- A waiver of authorization granted by an Institutional Review Board (IRB) or

Privacy Board; or

- “Limited Data Sets,” which include fewer identifiers and may be used under a Data Use Agreement for research and public health purposes.

In comparison to GDPR, HIPAA is less restrictive with regard to the secondary use of data after it has been de, identified but is less detailed as it is not applicable to entities outside the healthcare ecosystem, e.g., consumer health apps, wearables, and AI startups unless there is a contractual link.

DPDP Act: A Consent, Centric but Evolving Framework

India's DPDP Act, 2023 is a consent, driven framework and does not differentiate data into sensitive and non, sensitive categories as GDPR does. Health data is considered personal data, but its secondary use is mainly regulated through the rules of consent, legitimate use, and government exemptions.

Secondary processing for research is allowed by Section 4(2), which permits processing for "public interest, " inter alia research, statistical purposes, or archiving, if such processing does not result in decisions that directly affect the individual. On the other hand, the Act is silent on detailed provisions in the areas of pseudonymisation, anonymisation metrics, or ethics oversight, which are aspects where GDPR and HIPAA are more explicit.

The DPDP Act defines Data Fiduciaries and Significant Data Fiduciaries, who rather than being the data subjects, have been endowed with obligations such as impact assessments and audits. However, the extent of the GDPR DPIA framework is still somewhat wider than that of this Act. Rules regarding cross, border data transfer are still to be announced, thus causing the potential for uncertainty localizing collaborations in health research and AI.

An important indeterminacy is the extensive exemption for the State in Section 17, which may leave the door open for processing health data without consent for research purposes that are in line with 'public interest' thus giving rise to concerns as far as proportionality and transparency are concerned.

Comparative Observations

Considering all three legislations, GDPR is the most comprehensive and structured with a strong focus on rights, HIPAA puts emphasis on de, identification and sectoral compliance, and the DPDP Act can be viewed as an emerging framework with consent at the core and the safeguards gradually being developed. All of these point to the international challenge of not jeopardizing privacy while making use of the enormous scientific value that secondary use brings to the table and especially in times of AI, driven healthcare innovation.

Key Conflicts in Secondary Use Across GDPR, HIPAA, and the DPDP Act

The use of medical data for research and the creation of AI using such data is a major regulatory challenge when looking at rules like GDPR, HIPAA and India's Digital Personal Data Protection (DPDP) Act. Although all three systems have the same goal of protecting patient privacy, their philosophies, consent models, coverage of protections, and even technical requirements for compliance vary dramatically. The result of these differences is that companies running health tech platforms, conducting clinical trials across different countries, or using AI models trained on global health data sets face significant conflicts.

Divergent Consent Requirements and Legal Bases for Processing

The most significant issue is the one that points to the differences in the consent frameworks for the secondary use of data. According to the GDPR, health data falls under the category of 'special category data' and as such, any secondary use would require an explicitly informed consent unless a duly substantiated research exemption as per Articles 6 and 9 is invoked. In cases where consent is not required, the GDPR still requires the undertakings pursuant to the processor to implement strict measures such as pseudonymisation and obtain approval by the ethics committee. And just the opposite, HIPAA allows a determination that once data are de, identified using the Safe Harbor or Expert Determination methods, they are no longer under HIPAA's purview and can be used or shared without patients' consent. On the other hand, research involving limited datasets can be carried out if there is a Data Use Agreement. This leads to a fundamental conflict, de, identified data is still considered data that can potentially lead to privacy risks by GDPR, whereas HIPAA regards it as practically outside the privacy framework.

DPDP Act is basically a model based on consent. It requires users to be informed of purposes and give a clear and specific consent when their personal data are processed. The law also allows exemptions to be made for research but only the extent and procedural safeguards for covered work are left unspecified. What causes the most confusion for Indian researchers is the absence of a detailed research exception architecture in the Act which shortens and complicates their cooperative work with institutions from the EU and the US. Consequently, there exists the problem of three different and inconsistent domains of consent to be followed by entities: strict (GDPR), conditional (DPDP), and permissive (HIPAA).

Conflicting Standards for Anonymization and Re, identification Risk

Another point where the core conflicts arise is that of the diverse standards for the anonymization of medical datasets. According to the Safe Harbor provision under HIPAA, there are 18 types of identifiers that have to be removed from the data that is to be considered de, identified. Besides that, Expert Determination alternative way of doing that allows a qualified statistician to quantify the re, identification risk is "very small." However, GDPR opt for a tougher and more flexible technologically approach: data that is only pseudonymized is still regarded as personal data and real anonymization is nearly impossible due to the existence of modern re, identification methods. This high criterion is a product of EU's rights, based policy, i.e. the emphasis being on privacy risks to the individual in the future.

The DPDP Act refers to 'anonymised data' but does not provide technical or legal standards that can be compared with those of GDPR or HIPAA. The lack of detailed rules causes compliance issues for organizations that intend to utilize Indian health data for AI training or research purposes. Besides that, given the increasing global concern about model inversion, linkage attacks, and re, identification through auxiliary datasets, the discrepancies in anonymization standards among different jurisdictions pose substantial operational barriers. Data that are considered fully de, identified in the US may still be subject to GDPR requirements in Europe, thus making cross, border research more complicated.

Cross, Border Data Transfer Restrictions

These three systems also have major disagreements over the permissibility of cross, border transfers for research and AI. GDPR is very restrictive about transfers and only allows them to countries with adequacy decisions or when certain safeguards like Standard Contractual Clauses are in place. On the other hand, HIPAA stipulates that contracts with safeguards are required when identifiably data are being shared with an overseas business associate, but once data are de, identified there are no location restrictions. The DPDP Act, on the other hand, follows an 'allow, all, unless, restricted' approach, whereby cross, border transfers are permitted unless the government issues a notification that certain countries are restricted. This situation causes regulatory uncertainties since the restricted countries' list has not yet been made public. Thus, the ambiguity poses operation and compliance challenges for companies dealing with global AI models trained on Indian medical data.

Algorithmic Accountability and Governance of AI Training Data

Another point of disagreement that the four regulatory frameworks have regarding the issue of oversight is AI models trained using secondary medical data. The GDPR directly regulates automated decision, making, profiling, and requires impact assessments for high, risk processing. Hence, it indirectly controls the use of sensitive data for AI training. HIPAA does not have any direct provisions for AI regulation and instead, concentrates on the privacy and security of identifiable health information. Thus, after the data has been de, identified, AI model developers in the US are hardly subjected to regulatory oversight. Same goes with the DPDP Act which doesn't have explicit provisions for algorithmic accountability, automated decision, making rights, or mandatory impact assessments, thus leading to a gap when India is quickly digitally health expanding. This mismatch in regulations makes it hard for AI to collaborate globally, as a model trained in the US might not be able to meet the EU privacy standards.

Challenges for Harmonization in Global Health & AI Research

The endeavor to align regulatory standards that govern the reuse of medical data for research and AI is confronted by a range of obstacles of a structural, philosophical, and technological nature beyond geographical boundaries. The GDPR, HIPAA, and India’s DPDP Act are reflective of differing legal traditions and policy objectives at their core, thus making it very difficult for health research institutions that operate globally, pharmaceutical companies that have a worldwide presence, and AI developers to interoperate.

Differing regulatory philosophies present a major challenge. The GDPR is a comprehensive data protection model based on human rights, which is very much in line with individual autonomy, requiring explicit consent and providing strict safeguards for health data that are regulated by Articles 6 and 9. On the other hand, HIPAA is a sector, specific legislation that applies only to "covered entities" and "business associates" and permits the use of de, identified or "limited data sets" for research to a large extent without restrictions. The DPDP Act is a consent, centered but still maturing framework that places the burden of data protection on data fiduciaries but lacks the detailed protections and exceptions such as those of GDPR and HIPAA. These different starting points cause friction as they result in different standards concerning consent, de, identification, and allowable secondary uses. Thus, those engaged in AI research at the multinational level have to come up with different compliance strategies for each regime, which is a huge operational challenge.

Besides, the disparity in anonymization and de, identification standards is another big hurdle. According to HIPAA's Safe Harbor standard, data is considered "de, identified" once 18 specified identifiers are removed, thus giving a definite but somewhat outdated rule. GDPR, however, goes further and differentiates between anonymization (non, reversible) and pseudonymization (reversible with some additional data), having much stricter requirements due to the continuous development of re, identification methods. The DPDP Act recognizes anonymized data but barely provides legal guidance with regard to the threshold of anonymization, thus leaving the health, tech and research sectors in India in a state of uncertainty. Such discrepancies have led to the breakdown of cross, border data flows since what is deemed as sufficiently anonymized data under HIPAA may still be regarded as personal data under GDPR, thereby creating legal uncertainties for AI researchers who require huge datasets spanning different jurisdictions.

The next data transfer limitations at the international level make harmonization even more complicated. On one hand, the GDPR sets out some of the most stringent transfer controls such as adequacy decisions, Standard Contractual Clauses (SCCs), and restrictions related to Schrems II. On the other hand, HIPAA being a local health privacy law does not directly regulate international data transfers and is dependent on the presence of contractual obligations between covered entities and business associates for the regulation of such matters. As for DPDP, cross, border transfers are likely to be allowed, but there might be some restrictions or requirements for whitelisting, which have not yet been fully implemented. These transfer disagreements have led to bottlenecks in worldwide health research collaborations, such as clinical trials, genomic research, and AI training models. Research institutions have to go through a phase of local approval, contractual safeguards, and encryption or pseudonymization processes to share datasets in a legal way.

Moreover, the ethical tension between individual privacy and societal benefit is another reason why harmonization is difficult. The strictest standard imposed by GDPR for the processing of sensitive data mirrors the priority given to the rights of the individual and is, therefore, likely to slow down large, scale population research. On the other hand, HIPAA makes it easier for public health research to be conducted by providing more flexible de, identification approaches, but it may still be insufficient in addressing modern privacy risks, particularly in AI systems that are susceptible to model inversion attacks. India's DPDP Act tries to strike a balance but is missing specific research carve, outs or an independent health, data framework similar to the EU's clinical research regulations. Achieving harmonization implies being able to reconcile these opposing values in different legal cultures, which is a very difficult task owing to the factors of differing historical experiences, public expectations, and institutional capacities.

In addition, the emergence of AI healthcare tools complicates the situation even further. There are differing requirements regarding algorithmic transparency, data minimization, lawful bases for processing, and anti, bias safeguards for AI systems that are trained on medical datasets across different countries. GDPR's rules concerning automated decision, making and profiling impose heavy compliance requirements on AI developers, as these rules require that the decision made be explainable and that there is human oversight. HIPAA does not have any specific AI, related obligations in this regard, thereby leaving a lot of gaps in governance. On the other hand, DPDP Act is silent on AI, thus providing no guidance to companies working on the development of diagnostic algorithms or predictive models. The absence of harmonized standards makes it difficult for multinational AI projects, such as federated learning systems, cross, border disease surveillance tools, or global oncology databases, to be consistent in compliance and risk management.

Harmonization is also hampered by disparities at the institutional level. The EU boasts very advanced Data Protection Authorities (DPAs) that have vast experience in enforcement, whereas the enforcement of HIPAA is the responsibility of the United States Department of Health and Human Services. On the other hand, India's Data Protection Board is relatively new and still finding its feet. Differences in regulatory capacity, enforcement culture, and judicial precedent make it difficult for mutual recognition or standardized global frameworks to be implemented.

Last but not least, there are also different commercial incentives and data governance models that exist in different parts of the world. The U.S. is characterized by the vigorous involvement of the private sector in the healthcare data markets, while the EU mainly lays emphasis on public oversight and ethical safeguards. India's digital health ecosystem, which is growing at a rapid pace and is largely driven by the Ayushman Bharat Digital Mission, comprises the involvement of the state and the collaboration between the public and the private sectors. It takes more than just legal alignment to bring these different systems together; economic and institutional restructuring is also necessary.

In brief, the main factors that stand in the way of harmonization are legal philosophies that contradict one another, technical standards that are not always consistent, ethical dilemmas, challenges that are specific to AI, and institutional capacities that are unevenly distributed. Resolving these problems will take a lot of time and efforts on the part of all the nations involved in the process. They will have to work together continuously, come up with safeguards that are compatible with each other, and develop clearer guidelines with regard to anonymization, cross, border transfers, and AI governance.

The Way Forward: Pathways to Harmonization and Robust Governance

The secondary use of medical data for research and artificial intelligence (AI) provides a lot of positive impacts to public health, medical innovation, and evidence, based policy, making. However, the differing regulatory philosophies of GDPR, HIPAA, and India's DPDP Act make it difficult to coordinate research across borders, hinder the creation of large, scale health datasets, and cause development uncertainty of AI. In future, instead of uniform legislation (which is impracticable due to differences in jurisdictions), harmonization should be achieved through shared ethical principles, interoperable standards, and strong governance structures that facilitate scientific progress whilst respecting individual rights.

One of the ways to achieve harmonization is the use of interoperable anonymization and de, identification standards. The different standards for pseudonymisation in GDPR, Safe Harbor, and Expert Determination in HIPAA, and the DPDP Act's poorly developed framework for anonymization have significant differences. Such differences result in compliance costs increase and cross, border dataset pooling discouragement by researchers. The core of the solution is in global technical standards that would enable defining robust anonymization levels so that AI models re, identification risks would be minimal, and at the same time different legal regimes would be accommodated. These and similar organizations are well, positioned to guide the development of consensual standards that countries can implement voluntarily. Unified technical benchmarks would set data free from the constraints of the regulatory maze and still ensure uniform levels of protection.

The second pathway involves developing unified consent and participation frameworks that balance autonomy with the realities of large, scale research. The present consent model is unable to address the needs of modern research in which data can be reused, linked, and processed by algorithms for multiple future uses. In GDPR, scientific exemptions are supported, but legal processing has to be based on lawful bases and require explicit consent. HIPAA, on the other hand, permits broad research authorizations and IRB waivers. The DPDP Act in India is heavily focused on consent, thus long, term research repositories face practical problems. To reconcile these differences, dynamic consent, a model where participants can change their preferences, might be considered the best global practice. At the same time, broad consent along with strict oversight, audit mechanisms, and secure processing could also ensure that medical data are ethically reused. The aim is to grant power to individuals without imprisonment by beneficial research.

Third, enhancing accountability measures in GDPR, HIPAA, and DPDP is crucial to managing the risks posed by AI, powered secondary utilization of medical data. While GDPR already includes a mandate for the implementation of Data Protection Impact Assessments (DPIAs), HIPAA requires risk analyses and security assessments under its Security Rule. The DPDP Act places great responsibilities on data fiduciaries but does not provide for algorithmic accountability explicitly. The future governance frameworks in this area should not only be limited to the disclosure of algorithm use but should also encourage the deployment of bias testing, audit trails, and explainability mechanisms. These safeguards are vital given the novel privacy threats are coming with AI models such as model inversion, indirect memorization of patient data, and discriminatory outputs. The alignment in this aspect does not imply the need for strict regulatory uniformity but rather convergence based on principles, where respective accountability expectations are in sync even if procedural requirements vary.

Fourth, the regulation of cross, border data transfers needs to be updated so that it can facilitate responsible international research. The rigorous adequacy and contractual safeguard conditions of GDPR stand in contrast to the more liberal approach of HIPAA. India's DPDP Act is still at a stage where it is difficult to judge the compliance requirements for the future in the research and health tech sectors. The harmonized solution may consist of standard contractual stipulations particularly designed for research collaborations in the medical field, joint research agreements, and global health data infrastructures. Besides, International communities can foster mutual recognition contracts (MRAs) also for compliant research institutions which in turn would provide the trusted entities with ability of exchanging data under predefined security measures. Implementation of such steps will lessen the resistance, enhance the reciprocal trust and facilitate the global response to health crises.

Fifth, public trust should be the primary concern in the process of harmonization. Medical research and AI are reliant on the individuals' readiness to provide their sensitive health data. Transparency in data usage, the availability of grievance redress mechanisms, and the presence of accountability features are some of the ways through which societal trust can be built. Awareness programs explaining anonymization, research benefits, and patient rights can remove the apprehension and invite more volunteers. No matter how advanced a legal framework may be, it will never succeed if there is no trust.

Finally, harmonization efforts may look to international cooperative models such as OECD privacy guidelines, WHO health data governance frameworks, and global AI ethics principles for inspiration. These organizations offer impartial stages for the countries to work together without losing their sovereignty. A shared worldwide code for medical data reuse, comprised of ethical, legal, and technical principles, can serve as a bridge to link together GDPR's rights, based philosophy, HIPAA's sectoral approach, and India's emerging data protection landscape.

In brief, aligning medical data governance among GDPR, HIPAA, and the DPDP Act calls for multi, layered strategies: technical interoperability, flexible consent models, enhanced accountability, refined cross, border standards, and continued public trust. Through international collaboration and principled governance, the immense value of secondary medical data for research and AI can be unlocked without compromising the dignity, privacy, and rights of individuals worldwide.

REFERENCES

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

2. U.S. Dep't of Health & Hum. Servs., *Health Insurance Portability and Accountability Act of 1996* (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936.

3. U.S. Dep't of Health & Hum. Servs., *HIPAA Privacy Rule*, 45 C.F.R. pts. 160 & 164 (2023).

4. U.S. Dep't of Health & Hum. Servs., *HIPAA Security Rule*, 45 C.F.R. §§ 164.302–164.318 (2023).

5. Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

6. European Data Protection Board (EDPB), *Guidelines on Processing Personal Data for Scientific Research Purposes* (2021).

7. European Data Protection Supervisor (EDPS), *Opinion on the Use of Health Data for Research and Innovation* (2020).

8. Organisation for Economic Co-operation and Development (OECD), *Health Data Governance: Privacy, Monitoring and Research* (2019).

9. World Health Organization, *Ethics and Governance of Artificial Intelligence for Health* (2021).

10. U.K. Information Commissioner's Office (ICO), *Anonymisation, Pseudonymisation and Privacy Enhancing Technologies Guidance* (2022).

11. U.S. National Institute of Standards & Technology (NIST), *De-Identification of Personal Information* (NISTIR 8053, 2015).

12. M. Veale, Reuben Binns & Lilian Edwards, *Algorithms That Remember: Model Inversion Attacks and the Limits of Anonymisation Under the GDPR*, 36 Computer L. & Security Rev. 105 (2020).

13. Khaled El Emam & Luk Arbuckle, *Anonymizing Health Data: Case Studies and Methods to Get You Started* (O'Reilly Media 2013).

14. Lawrence O. Gostin & James G. Hodge Jr., *US Health Information Privacy: HIPAA and the GDPR*, 42 J.L. Med. & Ethics 693 (2014).

15. Meg Leta Jones, *The Right to Delete Under the GDPR: Implications for Health Research*, 9 Int'l Data Privacy L. 3 (2019).

16. R. Shankar & Smriti Parsheera, *Regulating Health Data in India: A Comparative Analysis with GDPR and HIPAA*, 12 Indian J.L. & Tech. 33 (2021).

17. Anita Allen, *Privacy in Health Research: A Comparative Study of Regulatory Approaches*, 48 Hastings Ctr. Rep. 25 (2018).

18. S. Wachter & B. Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of AI*, 2019 Colum. Bus. L. Rev. 494.

19. U.S. Food & Drug Administration (FDA), *Proposed Regulatory Framework for Modifications to AI/ML-Based Software as a Medical Device* (2019).

20. Ministry of Electronics & Information Technology (MeitY), Gov't of India, *DPDP Act Rules – Draft Framework for Consent, De-Identification and Data Processing* (2024).