ILE MULTIDISCIPLINARY JOURNAL

VOLUME 4 AND ISSUE 2 OF 2025

INSTITUTE OF LEGAL EDUCATION

ILE MULTIDISCIPLINARY JOURNAL

APIS – 3920 – 0007 | ISSN - 2583-7230

(OPEN ACCESS JOURNAL)

Journal's Home Page – https://mj.iledu.in/

Journal's Editorial Page - https://mj.iledu.in/editorial-board/

Volume 4 and Issue 2 (Access Full Issue on - https://mj.iledu.in/category/volume-4-and-issue-2-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2025
APIS – 3920 – 0007 | ISSN - 2583-7230

Published by
Institute of Legal Education
https://iledu.in

EVOLUTION OF DATA PROTECTION LAWS: FROM HIPAA TO GDPR

AUTHOR - BHAVYA SHEETAL, STUDENT AT AMITY UNIVERSITY, NOIDA
BEST CITATION - BHAVYA SHEETAL, EVOLUTION OF DATA PROTECTION LAWS: FROM HIPAA TO GDPR, ILE MULTIDISCIPLINARY JOURNAL, 4 (2) OF 2025, PG. 101-111, APIS – 3920-0007 | ISSN - 2583-7230.

ABSTRACT

The evolution of data protection laws reflects society's growing recognition of privacy as a fundamental human right in an increasingly digital world. Beginning with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 in the United States, data protection regulations initially focused on securing sensitive health information. HIPAA established standards for the handling of personal health data, emphasizing confidentiality, integrity, and availability. However, as digital technologies expanded and data collection became more pervasive, new legal frameworks were needed to address broader privacy concerns across different sectors.

This shift culminated in the enactment of the General Data Protection Regulation (GDPR) by the European Union in 2018, which marked a significant milestone in global data privacy. GDPR introduced comprehensive protections covering all types of personal data, giving individuals more control over their information and placing greater accountability on data processors and controllers. Key principles such as data minimization, consent, transparency, and the right to be forgotten have since set new global standards for privacy compliance.

This paper traces the progression from sector-specific laws like HIPAA to the all-encompassing framework of the GDPR, analyzing how legal, technological, and societal changes have influenced the development of data protection laws. It also examines the global impact of GDPR, including its influence on data protection regulations in other regions such as the California Consumer Privacy Act (CCPA) and India's Digital Personal Data Protection Act (DPDPA). Understanding this evolution is crucial for policymakers, organizations, and individuals navigating the complex landscape of digital privacy.

Keywords: Data Protection, HIPAA, GDPR, Legal Evolution, Digital Rights.

DEVELOPMENT OF HEALTHCARE PRIVACY REGULATIONS GLOBALLY

Healthcare privacy regulations have evolved hand in hand with the digitization of health systems & an increasing reliance on personal health data in clinical & research environments. Not only has the rise of EHRs transformed how patient data is documented, but even the application of AI in standards of care deliverables has made the preservation of health information content more vital than ever. At international level, jurisdictions have established legal frameworks to respond to this increasing demand, including ethical, legal, and technological aspects. This section describes the global evolution of healthcare privacy regulations, exploring significant historical developments and their contextual foundations.

Early Foundations: Medical Ethics & Legal Precedents

Traditionally, healthcare confidentiality was enforced through codes of ethics. The Hippocratic Oath instructs to respect patient privacy, one of the first acknowledgments of this principle. With medical practice increasingly formalised, particularly throughout the 20th century, professional ethical codes were expanded to encompass explicit pledges of patient confidentiality. But there were no legal

ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2025
APIS – 3920 – 0007 | ISSN - 2583-7230
Published by
Institute of Legal Education
https://iledu.in

standards that made those ethical obligations enforceable until the late 20th century when comprehensive privacy legislation began to come into being. The first wave of healthcare-specific privacy regulations preceded the massive digitalisation of patient records. Statutory privacy mechanisms became inadequate to protect data that are stored, transmitted, & processed electronically, & countries began to take notice.[1]

International Harmonisation & Emerging Challenges

These national frameworks differ in detail, but they share common themes: consent requiring, restricting purpose of processing, security of stored data, & transparency on data use. Yet regulatory fragmentation creates considerable challenges for multinational healthcare providers, notably with respect to cross-border data flows. To counter these problems, international organizations such as the World Health Organization (WHO) & Organisation for Economic Co-operation and Development (OECD) have released recommendations encouraging responsible data usage in health studies & AI. The goal of these efforts is to build interoperable frameworks that maintain privacy and also promote global health innovation. Healthcare privacy law has evolved with the curve of technological change, ethical standards, & public policy exigency. The founding rules of HIPAA to the expansive rights framework of the GDPR to the growing momentum in emerging economies has made healthcare data protection a global issue. Yet as AI & big data continue to transform medical practice, tending coherent, adaptive & ethically grounded privacy laws remains a major global challenge.[2]

HIPAA (USA): KEY PRINCIPLES & HEALTHCARE APPLICATIONS

The HIPAA, signed into legislation enacted by the United States Congress in 1996, is among the most expansive legislative initiatives aimed at safeguarding patient confidentiality in the online era. Originally implemented to enhance the portability of health insurance & reduce administrative burdens in healthcare, HIPAA has transformed into a comprehensive set of standards aimed at protecting the security & authenticity of PHI in an ever-more integrated & data-centric healthcare environment. In this article, we will discuss the key principles & regulatory components of HIPAA & its real-world applications in AI-driven healthcare.

Regulatory Scope & Structure

HIPAA generally applies to three types of entities: (1) entities that are covered (such as healthcare providers, health plans, and healthcare clearinghouses), (2) business associates (third-party service providers that handle PHI on behalf of covered entities), and (3) indirectly, their subcontractors. The Department of Health and Human Services (HHS) established a set of federal regulations to enact the law, which is enforced by the Office for Civil Rights. HIPAA has the following key rules:[3]

i. Privacy Rule (2003)
ii. Security Rule (2005)
iii. Breach Notification Rule (2009)
iv. Enforcement Rule (2006)
v. Omnibus Rule (2013)[4]

Key Principles

HIPAA's approach to privacy & data security is guided by foundational principles that have shaped healthcare data privacy practices in the US & influenced global debates.

i. Minimum Necessary Standard: HIPAA mandates that covered entities only utilize, employ, or reveal the "minimum necessary" PHI to achieve a given task. This principle ensures that unnecessary or excessive data processing is avoided, mitigating risks of exposure or misuse.
ii. Right of Access & Correction: Patients are entitled to view their personal medical records and ask for amendments if the information is inaccurate or incomplete. This principle promotes patient autonomy & transparency, critical in contexts where AI-based decisions might depend on longitudinal data.

iii. Notice of Privacy Practices (NPP): Healthcare professionals must give patients a Notice of Privacy Practices, explaining how their data will be used & their rights under HIPAA. This element formalises informed consent in relation to data processing, although it is often criticised for being too complex & legalistic for lay understanding.

iv. Risk-Based Security Management: The HIPAA Security Rule mandates that covered entities perform risk assessments and establish safeguards—administrative, physical, and technical—that correspond to the size and intricacy of their operations. Security measures like data encryption and multi-factor authentication are essential components, access logs, & firewalls are mandated to prevent data breaches.

Applications in AI & Digital Healthcare

As AI becomes increasingly integrated into US healthcare systems, HIPAA provides a foundational legal & ethical framework for regulating the associated data flows. Its real-world applications extend across multiple domains:

(i) Electronic Health Records (EHRs): HIPAA played a pivotal role in catalysing the adoption of EHRs, particularly through the HITECH Act of 2009, which incentivised providers to transition from paper records. EHRs are now essential to AI applications that rely on structured patient data for diagnostics, predictive modelling, & clinical decision support systems.[5]

(ii) Telemedicine: The COVID-19 pandemic significantly accelerated the adoption of telehealth. HIPAA's provisions were temporarily relaxed under emergency waivers, allowing the use of platforms like Zoom & Skype for patient consultations. Post-pandemic, regulators are re- evaluating permanent frameworks to ensure telehealth solutions remain secure & compliant.[6]

(iii) AI in Diagnostics & Predictive Analytics: AI algorithms trained on historical PHI can support clinicians in diagnosing diseases like cancer, diabetes, & cardiovascular conditions. HIPAA ensures that such uses are regulated under strict conditions, requiring de-identification or proper patient authorisation if identifiable data is used. Business associate agreements (BAAs) are required between AI solution providers & healthcare entities to formalise these relationships.[7]

Limitations & Criticisms

While HIPAA has its strengths, it also has significant limitations that have been the subject of scholarly debate among scholars, clinicians & privacy advocates.

(i) Limited Scope: HIPAA does not cover myriad health-adjacent entities, like wellness apps, fitness trackers or social media platforms. The fragmented coverage has left regulatory grey zones in the health data ecosystem.[9]

(ii) Technological Lag: Some have argued that the HIPAA framework is ill-equipped to address complex & core issues imposed by modern AI healthcare systems, such as those regarding algorithmic bias, AI explainability and secondary data use.[10]

(iii) Over-reliance on De-identification: HIPAA permits use & disclosure of de-identified data without any limitations. However, advances in re-identification algorithms have undermined this assumption, since de-identified data from multiple & large datasets can be safely re- identified.[11]

HIPAA continues to be the cornerstone of healthcare data privacy law in the United States. Its principles have also guided institutional practices, fostered patient trust, & granted a legal basis for further investments in digital health technologies. But HIPAA's ability to tackle emergent ethical & technical complexities is being tested as AI, machine learning & ever-present systems of data collection increasingly define the healthcare landscape. An inclusive, technology-neutral, forward-looking health data law is needed, one that not only modernizes the law but leaves the core protections of HIPAA intact while extending HIPAA's coverage & flexibility.

ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2025
APIS – 3920 – 0007 | ISSN - 2583-7230
Published by
Institute of Legal Education
https://iledu.in

COMPARISON: HIPAA VS GDPR

HIPAA & the GDPR are two of the most globally influential data protection frameworks yet they are built on fundamentally different approaches to privacy, security, & individual rights. HIPAA is industry-specific & applies only to health information, while the GDPR is a cross-sectoral, horizontal regulation & applies to all personal data. These divergences reflect two different legal cultures — one based on regulatory pragmatism & the other on fundamental rights. It offers a comparative examination of HIPAA and GDPR such across multiple dimensions related to healthcare & AI integration.

Scope & Applicability

HIPAA is applicable exclusively to specific categories of organizations known as "covered entities," which include healthcare providers, health insurance plans, and healthcare clearinghouses — & their "business associates" that process PHI on their behalf. As a result, a wide array of organisations engaged in the gathering or handling of health-related information (think mobile health app developers or makers of wearable devices) are not under the jurisdiction of HIPAA. These have a limited scope, which creates regulatory gaps — particularly in the emerging area of consumer health technology.[12] By contrast, the GDPR has a wide & extraterritorial application. It governs all data controllers and data processors processing personal information of individuals residing in the EU, regardless of the organisation is not based in the EU. In addition, GDPR governs all types of personal data, not just health data. The broad scope of the regulation ensures that organizations in the entire health data ecosystem are working with the same legal obligations.[13] However, perhaps the key difference is that HIPAA is narrower & applicable only to the health sector, while GDPR is wider, & pertains to the handling of personal information that can include health data.

Definition & Treatment of Health Data

HIPAA concerns itself with PHI — any recognizable health data that covered entities and business partners do or have. It also distinguishes PHI from de-identified data that are not under its jurisdiction. "Data concerning health" is classified by the GDPR as a special category of personal data and therefore requires heightened protections. In contrast to HIPAA, the GDPR acknowledges a broader range of privacy interests
— profiling, inference, & automated decision-making — & imposes stronger transparency & accountability obligations even for pseudonymised data. The main difference in scope is that GDPR applies to data that would be considered health data at a broad level which would create obligations without regard to potential identity on the processor.

Grounds for Data Processing

Processing of PHI is permitted under HIPAA without individual consent for certain purposes — care, compensation, and medical procedures. Consent is only needed for purposes outside these core functions, such as marketing or research not falling under exemptions. GDPR requires a legal foundation is required to handle all personal data, while clear consent is necessary for processing specific types of data — such as health information — unless exceptions apply such as the public interest or healthcare exceptions. It is significant that the GDPR secures a more rights-oriented approach on the matter of consent — the latter being more informed, granular & freely givens. Main Difference: HIPAA has strong reliance on regulatory permissions for key healthcare functions, while GDPR defaults to an explicit consent requirement unless specified conditions are met.

Individual Rights

HIPAA provides only a handful of individual rights. Patients may view their health records, request amendments, & obtain an account of disclosures. But there are no or limited rights to object, delete, or port data. GDPR also extends a wide range of rights — from *"right to be forgotten"* to information mobility, which all

ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2025
APIS – 3920 – 0007 | ISSN - 2583-7230
Published by
Institute of Legal Education
https://iledu.in

apply to (and often influence) stages of your data lifecycle, together with your proper to object to processing. Critical to this is that GDPR also provides protections against automated decision-making, especially in situations where these decisions hold substantial significant effects on individuals — which is a critical safeguard in AI-driven healthcare. The key difference is that while HIPAA grants the individual very limited rights, the GDPR grants far richer individual rights, including rights that reflect 21st century concerns around data-driven decision-making & algorithmic profiling.

Security Requirements

These rules differ greatly in structure, but both HIPAA & GDPR impose security-related responsibilities on any entities that process health data. HIPAA's Security Rule requires entities transformed to execute safeguards such as managerial, tangible (e.g., controlling access to facilities) & technical ones (e.g., encryption & access controls). Focus on one of risk management based the size and complexity of the organization play a significant role. The GDPR mandates that "suitable technical and organizational measures" are implemented to maintain a security level that corresponds to the risk, which includes techniques like pseudonymization and encryption, along with the capability to test these measures on a regular basis. It's important to remember that GDPR also incorporates the principles of privacy by design and by default, thereby imposing requirements for data protection must be implemented at the earliest possible stage in system development. GDPR is dynamic & focuses on embedding data protection in system design while HIPAA dictates operational safeguards that organizations must tailor to their environment.

Breach Notification

Under HIPAA, covered entities must inform individuals affected by a breach, and in certain scenarios, report to the Department of Health & Human Services (HHS) and the media if 500 or more individuals are involved. Notifications must be sent within 60 days of the breach being discovered. GDPR mandates that data controllers notify the relevant supervisory authority of a personal data breach within 72 hours of noticing it, except when the breach is not likely to pose a risk to individuals' rights and freedoms. Where the stakes are high, those impacted also need to be informed. GDPR notification is more rapid, includes risk to rights, while HIPAA includes number of affected individuals as the main consideration.

Enforcement & Penalties

Enforcement of HIPAA is predominantly administrative, with civil monetary penalties coming from the Office for Civil Rights at HHS. How Much Are the Fines: Fines range depending on the level of culpability, with annual dollar caps per violation type up to $1.5 million. There are more robust enforcement mechanisms under GDPR. Fines can be imposed by regulatory bodies in each EU member country can impose fines of up to €20 million or 4% of global yearly revenue, depending on which amount is higher. [15] There is broad consensus that the penalties under GDPR are a more effective deterrent & tool to ensure accountability. The Biggest Difference: GDPR imposes substantially greater fines & has a more intrusive enforcement regime than HIPAA. HIPAA & GDPR Paradigms of Data Protection the US Healthcare Compliance Law—HIPAA, vs the EU Data Rights & Privacy Law—GDPR; namely: HIPAA is purpose- built for healthcare compliance rooted in US administrative law, whereas GDPR is a purpose-built, human rights & civil rights-oriented, cross-sectorial law grounded in EU constitutional principles. With the expanding role of AI in healthcare, GDPR's well-rounded & adaptable approach provides better safeguards for individual rights & more processing data practices. Still, HIPAA is a basic building block in the US, & there's debate about whether it could be expanded or woven into a larger, GDPR-style law to fill in the gaps that already exist. Navigating, reconciling & harmonizing local with global frameworks will

be crucial for international health care collaborations & AI deployments.

EMERGING FRAMEWORKS IN OTHER JURISDICTIONS

With the expansion of digital healthcare systems globally, developing economies have made considerable strides towards enacting data protection regimes that balance privacy with technological development. Four important Global South players—India, China, Brazil, & South Africa—have established strong normative & legal frameworks adapted to their sociocultural, political, & technological environments. These frameworks follow global data protection trends, particularly regarding the statuses of sensitive health data, but also establish regulatory practices that are new & unique within the world of data protection.

India: DPDPA 2023

The DPDP Act enacted in August 2023 is India's long awaited first comprehensive legislation concerning digital data privacy. The Act was introduced after the landmark decision in the case of *Justice K.S. Puttaswamy v Union of India* [14], and applies to digital personal data, irrespective of whether such data has been collected in an online or offline format & digitised thereafter. That includes a framework centered on consent, necessitating that consent for data processing is free, informed, specific, and unequivocal. Data Fiduciaries must furnish Data Principals (individuals) with details pertaining to the purpose. of collection of data & the nature of processing & are mandated to have reasonable safeguards against data breaches. The Act enshrines the right to information, the right to correction & erasure of data & grievance redress, among key rights. The law also establishes a Data Protection Board of India to monitor compliance & resolve disputes. While "sensitive personal data" is not defined in the Act, health-related information is broadly viewed as belonging to high-risk categories that require enhanced protections. Although data localisation obligations have been loosened, cross-border flows can be limited to certain jurisdictions as notified by the centre. The Act seeks to balance the need for privacy with the drive for technological innovation that supports the vision for India lead in the domain of health technologies & artificial intelligence. [15]

China: Personal Information Protection Law (PIPL)

China's *Personal Information Protection Law (PIPL)*, which took effect on 1 November 2021, is the country's first omnibus privacy law & a key pillar of its wider data governance framework, together with the DSL & CSL. The PIPL establishes strict guidelines for the handling of personal data & sensitive personal information, the latter broadly including biometric & health-related information. Data controllers & processors (the same terminology can also apply to data handler) must obtain separate, informed consent for processing sensitive information & ensure compliance with data minimisation, transparency, & accountability principles. China's strategy is remarkable for its focus on data localisation. Operators of critical information infrastructure & processors of large quantities of personal data must keep this data in China. They will only be permitted if the transfers pass evaluation of security conducted by the CAC, a move that has raised alarms for international research & collaboration.[16]

Brazil: *Lei Geral de Proteção de Dados* (LGPD)

Brazil's LGPD, which went into effect in September 2020, created a unified legal framework regulating the handling of personal data across all sectors. Much like the GDPR, the LGPD is applicable to both public and private organizations, as well as to entities outside of Brazil, if they handle the personal data of individuals residing in Brazil. The LGPD categorises health data as sensitive personal data, thus imposed stricter protective measures & the need for a legal ground for processing. These legal grounds include explicit consent, compliance with legal obligations, protection of health in procedures undertaken by healthcare professionals or entities. The law provides people with rights to know, amend, anonymise & erase their data. It also requires organisations to

assign a DPO to assist in adhering to data protection regulations. Regulatory authority is exercised by the *"Autoridade Nacional de Proteção de Dados (ANPD)"*, which has published sector-specific guidance, among which the guidance concerning health data. Fines could reach 2% of the organisation's revenue in Brazil per violation, up to a maximum of 50 million Brazilian reais. LGPD does help with enabling responsible AI development on the healthcare domain but at the same much needed confidence in the public.[17]

South Africa: *"Protection of Personal Information Act (POPIA)"*

South Africa's POPIA, which took effect in July 2021, is among the most advanced data protection regulations in Africa. It is applicable to both public and private sector entities and governs the handling of all personal data, including "sensitive personal data," such as health-related information. POPIA is founded on principles including lawfulness, minimalism, purpose specification, security measures, and participation of data subjects. The legislation forbids the handling of special personal data without explicit consent, although there are some exceptions, particularly regarding medical treatment or public health scenarios. Individuals (data subjects) are entitled to access and amend their personal data, to refuse processing, and to file complaints with the Information Regulator, the official authority responsible for supervising and enforcing the law. Non-compliance with POPIA can result in administrative penalties of up to ZAR 10 million as well as criminal repercussions, including up to ten years imprisonment for serious offences. Its enforcement regime shows that South Africa is serious about protecting health data in an economy that grows increasingly digital.[18]

Comparative Reflections

These newly emerging frameworks represent various points of convergence:

(iv) Consent & Transparency: There is an overarching theme of informed consent and clear processing, particularly for sensitive health data, across all four frameworks.

(v) Rights-Based Frameworks: The laws give individuals enforceable entitlements to view, amend, and remove their information.

(vi) Regulators: Independent authorities (e.g., India's Data Protection Board, Brazil's ANPD, South Africa's Information Regulator) to establish oversight & accountability.

(vii) International Influence: The laws have international roots, with the GDPR largely influencing their development, albeit with local nuances.

But China is stricter on data localisation than Brazil & India, and its cross-border data transfer rules differ from both, which can hinder global interoperability in health AI systems. Countries including India, China, Brazil & South Africa have made considerable advances in developing data protection legislation better attuned to the complexities of a digital writ. Their respective frameworks find a middle ground between the demands of personal privacy, public health & technological innovation. Although varied in structure & enforcement, these laws, taken together, represent a global pivot toward harmonised, rights-based, & accountable data governance in health. As AI systems designed by these jurisdictions provide the roadmap for global health strategy in a digital age, transnational collaboration among these jurisdictions will be essential in determining what a fair & secure health future looks like.

SPOTLIGHT ON INDIA: DPDPA, 2023

The recent passing of the DPDP Act in India represents a milestone in the nation's legal development concerning the safeguarding of individual privacy. The DPDP Act seeks to create a uniform legal structure for the handling of digital personal information of individuals without binding itself to any particular legal theory, it is motivated, interalia, by the fundamental right to privacy, recognized by the

Supreme Court of India, as a constitutional right which is necessary to enable value-added use of the data in an environment that encourages innovation, entrepreneurship, & economic growth, while preserving individual autonomy.
For AI-based healthcare systems such as ours, the Act lays a significant regulatory framework, but it is not without its gaps & challenges.[19]
Genesis & Constitutional Foundation

The DPDP Act has evolved through a long & complex legislative history post the Supreme Court acknowledged that privacy is a fundamental right. The Puttaswamy judgment emphasized that informational Privacy is a crucial aspect of individual freedom as outlined in Article 21 of the Indian Constitution. The committee led by Justice B.N. Srikrishna was established, which in 2018 submitted a draft data protection bill. After much tinkering & debate in parliament & approvals from various stakeholders in the GDPR- oriented eco-system, the DPDP Act passed out as India's first standalone piece of legislation dealing with personal data protection in 2023.[20]

Scope & Applicability

The legislation regulates the handling of personal data in digital form, online or digitised after offline collection. Different from its predecessor laws, the DPDP Act is agnostic to technology & sector segments leaving the door open for coming including personal data operated in business systems of entities sectors such as health-tech startups, platforms for AI-based diagnostics & telemedicine programs. The Act also possesses extraterritorial reach, as it applies to data processing that takes place outside of India when it is related to the provision of goods or services to individuals located in India. This aspect is especially significant for Indian data subjects whose information is handled by international AI healthcare providers.[21]

Key Concepts & Definitions

(viii) Personal Data: *"Any data about an identified or identifiable individual in relation to or by virtue of such data."*

(ix) Data Principal: *"An individual about whom the personal data is processed."*

(x) Data Fiduciary: *"Data Fiduciary is the one (either public or private) who decides the purpose & means of processing."*

(xi) Consent: *"The Act makes consent the default legal basis for the processing of data, which must be free, informed, specific, & unequivocal."*

(xii) Data Fiduciaries of Significance: *"A subset of data fiduciaries that shall have additional responsibilities predicated on the scale & sensitivity of data processed."*

While the Act itself does not specifically classify health data as "sensitive personal data," it entrusts the Government with the authority to declare specific categories of data, including medical or biometric data, to require elevated standards of protection.

Rights of Individuals (Data Principals)

The DPDP Act contains a range of rights intended to empower individuals with control over their data:

(xiii) Right to Access Information.

(xiv) Right to Correction & Erasure.

(xv) Right to Grievance Redressal

(xvi) Right to Nominate.

While limited compared to GDPR, these rights provide an initial framework for claiming individual agency in digital health systems.

Obligations of Data Fiduciaries

Data processors must adhere to the following principles:

- Establish valid consent along with a notice informing the purpose and nature of data processing.
- Make certain data is utilized only for its stated purpose & not kept longer than needed.

- Take reasonable security precautions to protect against such breaches.
- In case of a data breach inform the DPBI and impacted individuals.

Additionally, other provisions apply to Specific Data Fiduciaries, & they would also be mandated to do a Data Protection Impact Assessment (DPIA), appoint a Data Protection Officer (DPO), & undergo periodic audit—all specific to AI applications processing bulk health data.

Cross-Border Data Transfers

In a significant change from earlier drafts, the DPDP Act does not impose general data localisation requirements. Instead, it allows cross-border data transfers to other countries or territories that have been informed by the central government. This governance model provides flexibility for global health data flows, while also enabling state intervention in the context of geopolitical or national security concerns.

Enforcement & Penalties

The Act creates the Data Protection Board of India as a quasi-judicial authority to oversee compliance, investigate breaches & impose penalties. In the nature of the breach and its severity, we can impose administrative fines that go up to ₹250 crore (about $30 million USD). But in contrast to GDPR, the Act also provides individuals a limited right to sue for compensation through civil litigation — leading to concerns about whether individual compensation mechanisms afford adequate redress.

Implications for AI in Healthcare

However, the DPDP Act has broad implications for AI-enabled healthcare systems:

(xvii) Dynamic Consent: AI systems working with personal health data need to be designed to capture & respect dynamic consent, particularly as models are updated or repurpose.

(xviii) Data Minimisation & Purpose Limitation: There are principles attached to algorithms that prevent the collection of unnecessary data, or the use of data for secondary purposes.

(xix) Security & Accountability: AI developers & health providers will have to maintain strict data protection protocols & restrictions for the protection of personal health data & may be designated as Significant Data Fiduciaries in cases where sizable datasets are being handled.

(xx) Despite the Act's promotion of transparency, it currently lacks measures for algorithmic explainability and audits for bias, factors important in the context of automated decision- making within the field of healthcare.

The Act is a shot in the arm for modernising the governance framework on digitalisation in India. It establishes a foundation for a consent-based, accountable, & secure data ecosystem, especially in critical domains such as healthcare. But for AI-led systems, the lack of dedicated provisions on algorithmic transparency, data ethics and profiling indicate that we will need either more regulation or complementary sector-specific guidelines. It will be crucial to align the DPDP Act with emerging global standards & ethical norms as India advances its digital health agenda, making possible the realisation of a responsible, rights-oriented future of AI in healthcare.

CONCLUSION

The journey from HIPAA to GDPR highlights a transformative shift in the global approach to data protection and privacy. Initially, laws like HIPAA were created to address specific sectorial concerns—in HIPAA's case, the protection of health-related information in the United States. It set foundational principles such as confidentiality, security, and individual rights within a healthcare context. However, the digital revolution introduced new challenges that traditional, sector-specific laws could not fully address. The rise of big data, cloud computing, and global data exchanges demanded a more comprehensive and harmonized framework.

The introduction of the General Data Protection Regulation (GDPR) by the European Union marked a pivotal moment in data protection law. Unlike HIPAA, GDPR is broader in scope, applying to all personal data regardless of sector. It redefined the roles and responsibilities of data controllers and processors while empowering individuals with enhanced rights over their personal information. Importantly, GDPR's extraterritorial reach influenced jurisdictions beyond the EU, acting as a catalyst for similar legislative initiatives worldwide.

The evolution from HIPAA to GDPR Illustrates a trend toward more unified, rights-based frameworks that recognize privacy as a universal human right. This progression reflects changing public expectations, technological advancements, and the growing complexity of data ecosystems. It also underscores the necessity for continuous legal adaptation to keep pace with innovation.

As data continues to be a valuable asset, the need for robust, transparent, and globally interoperable data protection laws becomes increasingly vital. The legacy of GDPR is already evident in new regulations such as the California Consumer Privacy Act (CCPA) and India's Digital Personal Data Protection Act (DPDPA), indicating a global shift towards standardized privacy protections. Ultimately, the evolution of data protection laws represents an ongoing effort to balance innovation with individual rights in an interconnected digital world.

Moreover, this legal evolution signals a growing consensus on ethical data use, accountability, and individual autonomy. Organizations are now expected not only to comply with regulatory requirements but also to embed privacy-by-design principles into their operations. This has led to a re-evaluation of data governance models, cybersecurity investments, and consumer trust strategies. As technology continues to advance—through AI, biometric systems, and the Internet of Things—the landscape of data protection will continue to evolve. Thus, future data protection frameworks must remain agile, forward-looking, and inclusive to address emerging risks while preserving individual freedoms. Policymakers, corporations, and civil society must collaborate to ensure that privacy laws remain relevant and effective in safeguarding digital dignity across the globe.

Endnotes

1 LUDWIG EDELSTEIN, THE HIPPOCRATIC OATH: TEXT, TRANSLATION AND INTERPRETATION 42 (Johns Hopkins Press 1943).

2 WORLD HEALTH ORGANIZATION, ETHICS & GOVERNANCE OF ARTIFICIAL INTELLIGENCE FOR HEALTH (2021); ORG. FOR ECON. CO-OPERATION & DEV. [OECD], RECOMMENDATION ON HEALTH DATA GOVERNANCE (2019).

345 C.F.R. § 160.103 (2024) (defining "covered entities" and "business associates").

4 U.S. DEP'T OF HEALTH & HUMAN SERVS., HIPAA PRIVACY, SECURITY, & BREACH NOTIFICATION RULES, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited Apr. 6, 2025)

5 Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, §§ 13001–13424, 123 Stat. 226 (2009).

6 U.S. Dep't of Health & Hum. Servs., Notification of Enforcement Discretion for Telehealth, HHS.gov (Mar. 30, 2020), https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

7 U.S. Dep't of Health & Hum. Servs., Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA), HHS.gov, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Apr. 6, 2025).

8 Nicolas P. Terry, Protecting Patient Privacy in the Age of Big Data, 81 UMKC L. Rev. 385 (2014).

9 Glenn Cohen et al., Ethical & Legal Implications of AI in Health Care, 322 JAMA 1031 (2020).

10 Latanya Sweeney, Only You, Your Doctor, & Many Others May Know, Tech. Sci. (2013), https://techscience.org/a/2015092903/ (last visited Apr. 6, 2025).

12 45 C.F.R. § 160.103 (2024).

13 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 3(2), 2016 O.J. (L 119) 1.

14 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

15 Digital Personal Data Protection Act, 2023, §§ 6–8, 17 (India).

16 Personal Information Protection Law of the People's Republic of China, arts. 28–30, 36–40 (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) (China).

17 Lei Geral de Proteção de Dados [General Data Protection Law], Law No. 13,709, arts. 5–11, 52 (Brazil).

18 Protection of Personal Information Act 4 of 2013, ch. 3, § 107 (South Africa).

18 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

19 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free & Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).

20 Digital Personal Data Protection Act, 2023, § 2 (India).