

Readiness for Smart Health Data Interoperability in the Maldives and India: A Doctrinal Comparative Analysis of Legal and Regulatory Frameworks

Raneeta Pal¹ and Ravi Kant²

HIGHLIGHTS

- Examines India-Maldives legal readiness for cross-border digital health data
- Compares India's enacted DPDPA 2023 with the Maldives' proposed privacy bill
- Identifies enforcement, cross-border transfer, and institutional capacity gaps
- Proposes a bilateral MOU and phased adequacy framework for data transfers
- Aligns findings with SDG 3, SDG 9, and SDG 16 for digital health governance

ABSTRACT

In the past few years, there has been a rapid digital transformation in the healthcare landscapes of countries in the Global South. Though these changes have created better opportunities and management, they have challenged the legal system regarding the security of health data. India and the Maldives are evolving in the digital health ecosystem; nonetheless, safeguarding personal health data is also a part of this evolution. It is imperative to ensure security in the era of AI-driven diagnostics, telemedicine, Health Information Exchange, and data transfer to other stakeholders for further treatments. This paper sets out to examine the legal readiness of India and the Maldives in managing digital health data, with a focus on identifying gaps and offering practical suggestions for improvement. The study uses doctrinal methods, where analysis of national health data laws, policies, judicial precedents, and academic papers from both jurisdictions is done. The paper reviews national data protection laws, such as India's Digital Personal Data Protection Act (DPDPA) of 2023 and the proposed Privacy and Personal Data Protection Bill, 2023; related healthcare policies, judgments, and expert opinions. India has made significant moves with the Ayushman Bharat Digital Mission, but concerns about data privacy, centralization, and transparency persist. The paper investigates the laws that facilitate cross-border data transfer and advocate harmony in digital health standards, uniformity in legal and healthcare professionals, and secure platforms for data transfer. The research alliance with Sustainable Development Goals (SDG) 3, which is good health and well-being, SDG 9, industry, innovation, and infrastructure, and SDG 16, peace, justice, and strong institutions. Along with this, it also aids digital transformation, adaptation, and securing smart solutions. Since India and the Maldives are strategic actors in the Indo-Pacific health data ecosystem, the right kind of legal infrastructure will accelerate the readiness for digital healthcare adaptation.

KEYWORDS

Digital Health Governance
Data Protection Law
Cross-Border Health Data
Innovation and Solution
Legal Framework

¹Raneeta Pal is an Assistant Professor at the School of Law, Mahindra University, Hyderabad, Telangana, India. Correspondence concerning this article should be addressed to Raneeta Pal. Email: pal-raneeta@gmail.com

²Dr Ravi Kant is an Assistant Professor at Symbiosis Law School, Pune, Symbiosis International (Deemed University), Pune, India. Email: dr.ravi9kant@gmail.com

INTRODUCTION

Background and Significance

Recent years have witnessed a notable shift in Global South's healthcare systems, with digital transformation being one of the notable aspects. India and the Maldives are progressively adopting Information and Communication Technologies (ICT) to improve quality of provision and accessibility of healthcare services. These countries have specific problems in healthcare, including limited access to healthcare facilities, shortage of human resources, and an ever-increasing demand for healthcare services (Sarwal et al., 2021).

The entire health care industry is in a digital paradigm shift, adopting new smart health technologies, AI-based diagnostics, telemedicine, and health information exchanges (HIEs). AI diagnostics offer early detection of diseases and facilitate tailored treatment plans. Telemedicine provides and serves patients remotely, which is beneficial to patients to access specialist healthcare services located in distant places. HIE improves the care of patients by enhancing the sharing of health information from multiple healthcare institutions, thereby improving the outcomes for patients. An example is India's Ayushman Bharat Digital Mission (ABDM), which aims to create an integrated digital healthcare platform that provides information to stakeholders on demand (Goh, 2024).

Even so, the rapid advancement of technology in healthcare services comes with serious concerns about privacy and security of personal health data. In addition to the sensitive nature of health information that is shared, there are strict laws that govern the rights of the patient, confidentiality, and privacy. In India, the Digital Personal Data Protection Act of 2023, prescribes rules for data processing and protection. Likewise, the Maldives' proposed Privacy and Personal Data Protection Bill, 2023 also includes provisions for the safeguarding of personal health information in relation to digital health (Ramdas et al., 2025). Regardless of these legislations, there are serious gaps regarding the enforcement and implementation of data protection laws dealing with the transfer of information and technology across international borders (Maleki Varnosfaderani & Forouzanfar, 2024).

As India and the Maldives continue to develop their digital health frameworks, there is a critical legal gap in the personal health data protection architecture that needs to be addressed and fortified. This requires not only amending current legislation, but also foundational policy to tackle governance issues of digital health in a globalized context.

In this study, the term 'health data' is specifically used to refer to the categories of information that are most relevant to the India - Maldives context. The data in ques-

tion include electronic health records of patients seeking specialised treatment in Indian hospitals, diagnostic test results, prescriptions, and medical histories which have to be transmitted across borders to ensure continuity of care. Telemedicine consultations and health insurance claims records are other data flow examples. While anonymised or aggregated data sets may likewise be traded for epidemiological research or the application of artificial intelligence-based diagnostics, this paper focuses on identifiable patient data exchanged for the direct provision of healthcare. Defining this scope helps to make a more precise legal analysis of the governance of the personal health data at a cross-border level.

Literature Survey

International digital health data governance

The global shift towards digital health systems has underscored the critical need for robust data governance frameworks. Countries worldwide are grappling with the dual objectives of leveraging health data for improved healthcare outcomes while ensuring the privacy and security of individuals' information. The European Union's General Data Protection Regulation (GDPR) stands as a benchmark, emphasizing individuals' rights over their data and imposing stringent obligations on data processors and controllers. Similarly, initiatives like the European Health Data Space Regulation (EHDR) aim to facilitate the secure exchange of health data across member states, promoting research and innovation in healthcare (Stevens, 2020).

In low- and middle-income countries (LMICs), the challenges are multifaceted. Limited resources, fragmented health information systems, and diverse health IT infrastructures hinder the development and implementation of effective data governance policies. A review of health information systems in LMICs highlights the pressing need for standardization, capacity building, and investment in health IT infrastructure to enhance interoperability and data governance (Jayathissa & Hewapathirana, 2023).

India's Digital Personal Data Protection Act 2023

The enactment of DPDPA in 2023 shows India's growing concern for protecting personal data. The Act emphasizes principles such as consent-based processes for data collection, data minimization, and limitation of purposes for which data is collected. It also establishes the Data Protection Board of India (DPB), which adjudicates on disputes and enforcements, as compliance is monitored (Ministry of Electronics & IT, 2023).

Some provisions within the Act have raised concerns, particularly the lack of portability and the proposed right to be forgotten. Leaving such critical rights out strips individuals of any real control over their data. Additionally, the Act allows the government a generous discretionary power in exempting government agencies from compliance, thus creating areas of concern for abuse of discretion and unaccountability (*Right to Be Forgotten: Applicable against Non-State Entities?* – Law School Policy Review, 2021).

Equally important is the DPDPA's stance on the transfer of data across borders. Just like other nations that participate in data protection, India is allowed to transfer data to those countries flagged as 'trusted', however, the criteria for trust remain undefined which can be detrimental to international partnerships and the free flow of data ("Cross-Border Data Transfer Requirements Under India DPDPA," 2025).

The proposed Privacy and Personal Data Protection Bill, 2023

The proposed Maldivian legislation is aimed at safeguarding the rights of individuals and handling of data more securely. This law specifies the functions of data subjects, data controllers, and data processors. The proposed Bill also emphasizes transparency, accountability, and responsible processing of personal data in the Maldives (Personal Data Protection Bill, 10th May 2026).

The progressive aspects of the Act are overshadowed by implementation challenges. Enforcement in the Maldives is hampered by weak institutional capacity and infrastructural limitations. In addition, the legislation does not provide unilateral definitions for cross-border data flows, leading to ambiguity in international data circulation.

Identified gaps in literature

One notable gap in the literature lies in the interoperability of health data frameworks and the legal provisions for cross-border data flow, particularly between India and the Maldives. Although both countries have framed data protection legislation, the lack of baseline provisions and the absence of mutually binding agreements stifle the free flow of data.

In addition, the literature is lacking from an angle of the South Countries, as no thorough research exists analyzing these legal frameworks in relation to the global South's normative frameworks and their impact on cross-border collaboration in healthcare. Filling out these gaps is important in enabling the creation of a digital health system that is bilaterally collaborative in nature while ensuring privacy and security of personal health data.

Research objectives

This study pursues three objectives. First, it reviews and analyses the health-data protection laws of India and the Maldives, with particular focus on India's Digital Personal Data Protection Act, 2023, and the proposed Privacy and Personal Data Protection Bill, 2023 of the Maldives. Second, it identifies gaps, inconsistencies, and challenges within the legal frameworks and practices governing health-data protection and digital health governance in both jurisdictions. Third, it proposes strategies for strengthening digital health-data governance and ensuring effective legal compliance in India and in the Maldives.

Research questions

This study is guided by three central questions. It asks whether significant similarities and differences exist between the health-data protection frameworks of India and the Maldives; whether legal, institutional, and enforcement gaps affect the governance and cross-border exchange of health data between India and the Maldives; and whether the existing legal and policy frameworks adequately support secure, interoperable, and legally compliant digital health-data exchange while protecting privacy and civil liberties. Ultimately, this research seeks to enhance adaptive and resilient legal systems that govern sensitive data within the dynamic landscape of digitalisation and globalisation.

METHODOLOGICAL APPROACH

Doctrinal Legal Research Methodology

The study is doctrinal and comparative in nature. The doctrinal part allows for detailed examination of the legislation, constitutional provisions and regulatory policies. The comparative dimension shows how the Digital Personal Data Protection Act, 2023, India, and the proposed Privacy and Personal Data Protection Bill, 2023, Maldives, are similar and different. In addition to the textual comparison, the analysis critically assesses the legal suitability of each digital health framework for digital health data in particular, the challenges of implementation (institutional capacity, enforcement mechanisms, and regulatory readiness) and the implications for governance of digital health in both jurisdictions. The analytical lens is primarily rights-based and oriented towards the protection of individual privacy and autonomy, and at the same time, it is informed by the governance perspective required for safe and interoperable health data flows. There is no empirical survey nor fieldwork performed; this is recognized as a deliberate methodological choice for em-

phasis on existing literature. It is vital when assessing the effectiveness of laws and policies for addressing issues that arise from digital health system interventions such as AI diagnostics, telemedicine and Health Information Exchange (HIE). The methodology uses legislative text, policy documents and secondary legal commentary to uncover the doctrines to provide critical governance of health data. Doctrinal framework can be developed and expanded upon through future empirical research.

Sources of Legal Authority

This research utilizes a variety of primary and secondary legal materials, to ensure meticulous attention is given to all aspects of the research problem.

Primary sources

The primary sources drawn upon include legislative texts, constitutional provisions, and regulatory and policy guidance. The principal statutes of concern are India's Digital Personal Data Protection Act of 2023 and the proposed Privacy and Personal Data Protection Bill, 2023 from the Maldives, which serve as the basic legal instruments for the protection of personal data within their respective territories. Relevant constitutional provisions, such as the right to privacy in India, are also considered to explain the legal framework and constitutional background concerning data protection. In addition, formal guidance, circulars, and regulatory commentary issued by relevant authorities, such as India's Data Protection Board, are examined to assess how the statutory provisions are being interpreted and applied in practice.

Secondary sources

The secondary sources comprise legal commentaries and treatises, scholarly articles, and policy documents and reports. Legal commentaries and treatises by writers of authoritative texts delve into data protection laws and their implications, providing analytical insight into the legal effects and principles underpinning the laws. Scholarly articles by other academics focus on issues of effectiveness, problems, and comparison of data protection in India and the Maldives, while policy documents and reports produced by government and other public organisations provide crucial background material on the enforcement of data protection laws, their effects, and policies to amend or revise existing laws.

Incorporating these materials allows the study to achieve a rich synthesis of the law-related aspects that regulate and govern the health care data. Such mastery is done for the efficient critique of the existing legal system

while simultaneously enabling the formation of well-informed suggestions that seek to ameliorate the legal preparedness regarding the digital health ecosystem.

COMPARATIVE ANALYSIS OF LEGAL SYSTEMS

India's Legal Structure

India's promulgation of the Digital Personal Data Protection Act (DPDPA) in the year 2023 indicates a strengthening landmark in the country's quest for comprehensive governance of data. The DPDPA is India's first and sectoral data protection law, which seeks to balance the rights of individuals and their privacy on one hand, and a flourishing digital economy on the other (*India Digital Personal Data Protection Act (DPDPA) 2023 Explained /Key Provisions & Impact*, 2023).

Strengths and weaknesses of the DPDPA of 2023

The DPDPA of 2023 has several notable strengths. It adopts a consent-centric structure, providing for the collection of consent from data principals before any processing of personal data occurs; these practices comply with international standards that enable individuals to retain control over their personal data (*A. (Dr) P. Mali, 2025*). The Act also establishes the Data Protection Board of India as an adjudicating entity mandated to monitor compliance and address challenges, an institutional mechanism that is important for the enforcement of data protection policies and laws (*What Is Data Protection Board under DPDP Law*, n.d.). In addition, the DPDPA has extraterritorial applicability, remaining applicable to entities based outside India as long as they process the digital personal data of individuals in India or data related to goods and services provided to them, thereby ensuring that even foreign companies managing Indian data remain compliant (*Data Protection Laws in India - Data Protection Laws of the World*, 2025).

The Act also has significant weaknesses. Perhaps the most controversial is the broad government exemption clause, which gives the central government freedom to exempt any of its agencies from the purview of the Act; such broad exemptions heighten the risk of misuse and lack of control, and in the digital health context this is significant because government health agencies and public health programmes, including ABDM itself, could fall within the scope of such exemptions, potentially placing large volumes of sensitive health data outside the Act's core safeguards precisely where patient trust matters most (Davis, 2025). The Act's scope is also limited, since it deals only with digital personal data and does not cover data that is not digitised unless it is later digitised; this narrow approach risks leaving a great deal of data-processing activ-

ity unregulated (Data Protection Laws in India, 2025), and is a meaningful gap for healthcare specifically, where paper records, physical diagnostic films, and offline patient intake at smaller clinics remain common, creating an uneven compliance landscape as India's health system digitises unevenly across urban and rural providers. A further weakness lies in the ambiguity surrounding cross-border data transfers: although the Act allows transfers to designated countries, it does not provide clear grounds for such designations, which may impede overseas business and international data flows; for India-Maldives health data exchange specifically, this means Indian hospitals treating Maldivian patients currently operate without settled criteria for what would qualify the Maldives as a 'trusted' jurisdiction under Section 16, a gap this paper returns to in the Recommendations section (Qureshy & Khan, 2024). Finally, certain rights have not been provided for; data portability and the right to be forgotten are examples of rights that the DPDPA does not expressly provide, which limits an individual's control over their data. This omission is particularly consequential for health data, since, without portability, patients moving between hospitals or health systems, including across the India-Maldives corridor, cannot easily transfer their own diagnostic and treatment histories, undermining the continuity of care that HIE systems are meant to enable (P. Mali, 2018). Taken together, these are not merely theoretical legal gaps but carry practical implications for the interoperability of cross-border digital health systems: broad exemptions and unclear transfer conditions create legal uncertainty for institutions establishing HIE infrastructure, while the absence of portability rights undermines the continuity of care that AI diagnostics, telemedicine, and HIE are meant to facilitate.

The Implementation and Impact of Ayushman Bharat Digital Mission (ABDM)

The Ayushman Bharat Digital Mission (ABDM) is an initiative by the Indian government to digitize the healthcare system in India, launched in 2021. It aims to integrate the healthcare silos in India and improve access and portability of health records for the citizens (Sharma et al., 2023).

Implementation of ABDM has centred on three core components. A unique Health ID allows Indians to gain digital access to their health records and eases access to those records across healthcare practitioners. The initiative also engages hospitals, clinics, and diagnostic laboratories to enroll in the digital system, improving interoperability and the exchange of healthcare information. Underpinning both is an e-health framework comprising an assemblage of categorised digital health records, data,

telemedicine frameworks, and public health registries that are intricately linked and secured within a regulated 'e-health' perimeter.

ABDM has made significant progress in e-health adoption in the healthcare system, including the introduction of QR-codes for OPD registration. Patients no longer need to fill out paper forms or wait for staff to assist, making the process more streamlined. In addition, the Mission has improved data management processes, which contribute to better policies in resource allocation and strategic spending.

Nonetheless, issues still exist. The gap in digital skills and literacy in different areas poses difficulties in uniform adoption. In addition, these issues are further aggravated in the absence of protective measures and well-defined legal frameworks due to uneasiness regarding data privacy and security (Ministry of Health and Family Welfare, 2021).

Public and Expert Opinions on Data, Privacy and Security

The focus of discussion has shifted concerning data privacy and security with reference to expansive digital programs like ABDM in India.

A considerable segment of the population shows apathy regarding the safety measures of data collected from them. Trust in digital services and platforms has already been eroded due to high-profile data breaches and concerns about surveillance. The lack of transparency with regard to the data practices used aggravates the issues (*Countering Disinformation Effectively*, 2024).

Cybersecurity specialists focus on large-scale and systemic vulnerabilities concerning digital health. The massive scale of sensitive health data could prove disastrous if exposed due to insufficient protection, making it a prime target for hostile entities. Experts suggest tight security, periodic audits, and extensive campaigns to raise awareness of the data security risks to reinforce the security of sensitive data.

In addition, there is a marked absence of well-defined legal boundaries to distributing roles, assigning responsibilities, and establishing frameworks for the modality of grievance redressal. Attention is further drawn towards the incorporation of privacy-by-design to avert contravention of crucial legal frameworks.

Although the Digital Personal Data Protection Act of 2023 and the Ayushman Bharat Digital Mission mark milestones in India's journey toward digitization and data security, their effectiveness will be determined by the action taken on the ground, constant monitoring, and involvement with relevant parties. Actively resolving the noted challenges and promoting accountability will be

critical in accomplishing the intended advantages of these initiatives (Ministry of Health and Family Welfare, 2023).

Maldives' Legal Framework

Review of the proposed Privacy and Personal Data Protection Bill, 2023

The Maldives initiated the drafting of the Personal Data Protection law in 2021, and a revised version was opened for public comment in 2023. Maldives marked an important milestone in the creation of a legislative structure on the privacy and protection of personal data. Consistent with the intent, the proposed bill seeks to restrict the collection, processing, and disclosure of information to ensure the rights of individuals are respected while allowing reasonable management of data by organizations (Ministry of Tourism and Environment, 2023).

Key features of the proposed Bill include its scope and applicability, data subject rights, and responsibilities for data custodians and processors (Bentotahewa et al., 2022). Like many other data protection laws, the proposed Bill applies to both public and private entities as well as individuals who process personal data in the territory of the Maldives. It grants data subjects rights such as accessing their data, correcting their data, and withdrawing consent, while placing responsibility on organisations that handle personal data to take reasonable measures to protect that data and ensure accountability for its security.

The proposed Bill has notable strengths and challenges. Its strengths lie in its compliance with global requirements, since its similarities with the laws of other countries aid compliance and support the standardisation of international data flow, and in its holistic approach, which attempts to address a plethora of data-processing concerns and thus resolve data privacy issues more exhaustively. Its principal challenges concern the enforcement framework, which needs further groundwork on compliance and rectification processes to avoid unnecessary delay in punitive procedures, and public awareness, since it remains vital to ensure that businesses and individuals understand their responsibilities and duties under the proposed Bill.

Digital Health Initiatives in Focus: Achievements and Obstacles

Additional to the Bill, the Maldives has recently embarked on a comprehensive digital governance initiative called Maldives 2.0, a three-year national digital transformation program launched in 2025, structured into eight strategic pillars covering various areas of digital gover-

nance, such as digital identity, secure and sovereign infrastructure, and interoperability of government platforms. At the heart of this program is the eFaas digital identity system, which is accompanied by a draft Digital Identity Bill that provides the legal framework for secure digital identity verification in public and private services, such as in healthcare (Liang, 2026). In addition to social security services and banking, authorities have singled out healthcare as a service that the citizens will be able to access remotely when the integrated digital identity system is in place, minimising the need to travel to another island to receive care. A parallel draft Cybersecurity Bill would create a National Cyber Security Agency, adding a baseline security standard for public institutions, including health data systems. Such efforts are a positive development towards Digital Public Infrastructure (DPI) that will enable secure and integrated digital health systems. A UNDP policy assessment in 2025 however, concluded that the Maldives still did not have a unified government system architecture that establishes common services and interoperability standards, with individual government departments, including health authorities, still developing systems with limited interoperability (*Digital transformation*, 2025). This gap reinforces the paper's broader argument, whether legal readiness for digital health governance depends not only on data protection legislation but on the DPI, identity infrastructure, and cross-agency interoperability standards that the Maldives 2.0 aims to build (Bentotahewa et al., 2022).

Progress under the Maldives 2.0 can be seen in the construction of a national digital health blueprint, a landmark milestone that sets a foundation for the adoption of innovative technologies in healthcare service delivery, and in the ongoing implementation of Electronic Medical Records (EMR) systems in public health facilities to enhance interoperability and health information exchange. Nonetheless, obstacles remain. The geographical dispersal of the Maldives' islands poses challenges to providing uniform digital infrastructure nationwide, while inadequate technical training means participants require more advanced skills. The accuracy and reliability of health data remain important for informed decision-making and policy formulation, and, despite progress under the Maldives 2.0, the fragmented government system architecture, with no unified interoperability standard across agencies, means health data systems risk being built in isolation from the broader digital identity and data-exchange infrastructure now under development (*Maldives 2.0*, 2025).

It is important for the Maldives to be moving towards the creation of legal frameworks for data protection, alongside beginning work on other domains of digital health. These frameworks are important, but will have no constructive outcome without the execution, participa-

tion of relevant stakeholders, and the continual efforts to address infrastructure and capacity challenges.

Cross-jurisdictional Comparison: India and the Maldives

Similarities and differences in legal frameworks and enforcement mechanisms

Both India and the Maldives have developed legislative frameworks for the protection of personal data, signifying an advance in privacy and data protection. India's Digital Personal Data Protection Act, 2023 (DPDPA), corresponds with the Maldives' proposed Privacy and Personal Data Protection Bill, 2023, reflecting their respective approaches to data protection.

Both frameworks share several features. They require consent-based processing, whereby personal data may be processed only after prior, explicit, and unequivocal consent from the individual concerned, and they grant data subjects rights to access, rectify, and revoke previously granted consent. Both also impose obligations on data handlers to maintain internal operational policies that provide appropriate administrative and technical safeguards ensuring openness, data security, and protection, with the proposed Bill similarly requiring compliance with its rules.

The two frameworks diverge, however, in several respects. India has created the Data Protection Board to supervise compliance monitoring and grievance redress, whereas the Maldives' proposed Bill provides for a privacy commissioner whose operational and enforcement capacity is still emerging. Their scope and applicability also differ: the DPDPA applies to personal digital data and has extraterritorial reach over entities outside India that process the data of Indian individuals, while the Maldives' proposed Bill is applicable domestically and concentrates on data-processing activities occurring within Maldivian borders. Their enforcement mechanisms differ as well, since the DPDPA outlines specific monetary penalties for non-compliance, whereas the Maldives' proposed Bill also contains punitive provisions but suffers from a lack of definitional clarity that could hinder its effectiveness.

Examination of regulations and agreements on cross-border data transfers

India. The DPDPA allows for cross-border data transfers unless a country is listed on a government-issued "negative list." This policy has some advantages and disadvantages. On one hand, it provides some leeway, but on the other, it allows the government a lot of latitude in determining where data can be exported. There is currently

no published negative list that consigns organisations to limbo regarding compliant data transfer solutions.

Maldives. The Maldives' proposed Bill is concerned with cross-border data transfers by stipulating that personal data may only be transferred to other jurisdictions that provide an adequate legal framework for data protection. However, the proposed Bill is vague with respect to adequacy criteria and the methods for recognition of such jurisdictions, thus creating challenges for its practical implementation (Crawford & Lee, n.d.).

Bilateral agreements. As of now, there is no specific bilateral agreement between India and the Maldives that addresses the issue of cross-border data transfers. Both countries have, however, shown a willingness to enhance collaboration on digital infrastructure and services, which could lead to agreements facilitating the exchange of data while ensuring adequate privacy and security (*Maldives / Jurisdictions*, 2023).

Evaluation of interoperability and recognition of legal standards

The Maldives' proposed Bill has limited interoperability with India's DPDPA because of divergences in the underlying legal systems and enforcement frameworks. While both legal frameworks have some common principles, including processing by consent, data subject participation, the absence of basic uniform criteria on cross-border data transfer, and the lack of mutual recognition agreements pose obstacles to data exchange.

The OECD (Organization for Economic Co-operation and Development) comments explicitly with regard to the interoperability in the data protection system with data circulated between borders, highlighting the maintenance of data privacy protection standards. Equivalence in legal frameworks, mutual acknowledgment of data protection adequacy, and collaboration between the regulatory bodies' frameworks make interoperability possible (*Interoperability of Privacy and Data Protection Frameworks*, 2021). For India and the Maldives, investigating interoperability may involve the creation of mutual recognition agreements, through which each country formally acknowledges treaties or agreements governing the lawful transfer of data under the other's data protection mechanisms; the harmonisation of legal frameworks, through the reconciliation of definitions, principles, and enforcement approaches to build trust and reduce legal uncertainty across jurisdictions; and the building of institutional capacity, since protecting data across both countries in line with agreed standards requires fortified institutional capacity to enforce data protection laws (PIB, 2015).

Along these lines, both India and the Maldives would be able to pursue enhancing the frameworks in data pri-

vacy, enabling greater inter-jurisdictional data flow while protecting the privacy of individuals.

ISSUES AND SHORTCOMINGS IN EXISTING LEGAL STRUCTURES

Legal Shortcomings

Critical issues remain unaddressed by the legal frameworks available in India and in the Maldives regarding enforcement mechanisms, emerging technologies, and cross-border data flows, even as legal provisions on data protection are being constructed (Gaur, 2025).

Outdated Emerging Technology Provisions in Health Data Protection Legislation

The intent behind India's DPDPA 2023 and the Maldives' proposed Privacy and Personal Data Protection Bill were to protect personal data in the digital sphere, but several of their core provisions expose gaps when read against the demands of AI diagnostics, telemedicine, and HIE specifically.

On consent, DPDPA Section 6 requires that consent be free, specific, informed, unconditional, and unambiguous - a standard built for discrete, one-off data collection. It does not clearly address the layered consent that AI diagnostic tools require, where a single dataset may be reused for algorithmic training, real-time clinical decision support, and retrospective research, each raising the question of whether the original consent still applies.

On cross-border transfer, DPDPA Section 16 permits transfers to any jurisdiction by default unless the central government notifies a restriction – a negative-list model with no published restricted-country list to date. This provision is too permissive when considering the requirements of AI-enabled health applications, which demand advanced data protection protocols for the safety and privacy of patients (Panchal, 2024), since it leaves hospitals and HIE operators with no positive criteria for assessing a receiving jurisdiction's health-data safeguards before a transfer takes place.

On exemptions, Section 17 exempts government processing carried out in the interest of state security, and separately exempts research, archiving, and statistical processing under Section 17(2)(b), provided the processing does not inform a decision about a specific individual. Both are relevant to digital health: the state-security exemption could, in principle, extend to government-run health programs and registries, while the research exemption bears directly on AI-diagnostic model training, yet neither carve-out specifies additional safeguards tailored to the sensitivity of health data.

The Maldives' bill raises a parallel concern on the

transfer side: its cross-border provision requires an assessment of "adequate" protection in the receiving jurisdiction but, like DPDPA Section 16, does not specify the criteria or process for that adequacy determination (Panchal, 2024).

Outstanding Gaps in Comprehensive Frameworks Governing Cross-border Data Sharing

Both countries' data protection regulations allow for cross-border data transfer, but there is no explicit structure on how to manage (govern) those transfers. The DPDPA allows for the sharing of personal data outside the borders of India until the government specifically restricts certain regions. The Maldives proposed Bill similarly states that personal data may only be sent to those jurisdictions that provide an adequate level of data protection for personal data. In both scenarios, there is no statutory provision that determines how the adequacy of data protection will be assessed, granted, and formally recognized. The lack of clarity in these laws results in inconsistent practices and inadequate measures to safeguard sensitive health information exchanged across borders (Qureshy & Khan, 2024).

Institutional gaps and the enforcement framework gaps

Institutional inadequacy and a lack of sufficient enforcement frameworks hinder the enforcement of the data laws. In India, the DPDPA allocates to the Data Protection Board the responsibility of monitoring compliance and grievance handling. It has been noted, however, that there are gaps with regard to the Board's autonomy, enforcement mechanisms, and outcomes. While the proposed Bill in the Maldives provides for the creation of a privacy commissioner, the mechanisms for enforcement are inactive. Such inadequacies hinder the effective enforcement of data protection laws and the safeguarding of personal health information (*Data Protection Laws in India*, 2025).

Impacts on the Ecosystems of Digital Health

In the healthcare sector of India and the Maldives, the rapid adoption of digital technologies brought several advantages, such as expanding accessibility and improved efficiency. However, there are several outdated legal challenges that impact the digital health ecosystem.

Impacts of Legal Ambiguities on the Provision of Health Services and Innovation

The absence of an elaborate law for protecting information creates an enigmatic gap of legal ambiguity regarding

data collection and storage practices, which may impede the adoption of new digital health initiatives. The Digital Personal Data Protection Act, 2023 has been brought into force in a phased manner pursuant to the Central Government's commencement notification dated 13 November 2025. While provisions relating to the establishment and functioning of the Data Protection Board of India are operative, several substantive provisions imposing data-protection obligations are subject to a later commencement date under the phased implementation framework. The bigger question is whether it will be able to fully address issues arising from advanced technologies such as artificial intelligence and telemedicine. The same can be said of the proposed Privacy and Personal Data Protection Bill, 2023, which equally fails to address the incorporation of these technologies thereby endangering the stagnation of innovation and new healthcare service provision.

Issues Relating to Privacy Violations and Risks of Data Breach

The absence of legal guidelines increases the risk of data breaches with encroachment of privacy tools. Weak enforcement accompanying established parameters may render healthcare practitioners ineffective in executing data security systems rendering patient files vulnerable to unauthorized access by third parties. Loss of trust arises among patients and exposing healthcare institutions to legal liability and reputational damage (Group, 2025).

Problems in Achieving Interoperability and Seamless Data Exchange

The holistic exchange of health data within systems and across geographies enables the digital health ecosystems to function effectively. Limited legal interoperability frameworks stifle data exchange across systems and countries due to a lack of legal provisions for interoperability. Such fragmentation may lead to inefficient care delivery, enduring patient backlog, and problems providing coordinated care in a multi-national environment (Holmgren et al., 2023).

The existing legal boundaries of these countries, India and the Maldives, pose obstacles that may stunt the growth and impact of digital health ecosystems for the Maldives and India. Solving these problems demands innovative, legal privacy boundaries for users, and up-to-date health data exchange governance frameworks, balancing patient privacy, health data innovation, and comprehensive legal protections (Alonso et al., 2023).

Alignment with Sustainable Development Goals (SDGs)

The frame of governance within the digital health data boundary in India and the Maldives, particularly under the provisions of The Digital Personal Data Protection Act, 2023 (DPDPA) for India and the proposed Privacy and Personal Data Protection Bill, 2023, is critical for moving towards aligning governance frameworks with United Nations Agenda 2030 Sustainable Development Goals (SDGs). However, as it stands, those provisions pose difficulties that fully comply with SDGs 3, 9, and 16 (*Understanding the Digital Personal Data Protection Act (DPDPA) 2023 / Tricog Health, 2024*).



Figure 1. Aligning governance framework with the SDGs

Contribution to SDG 3: Good Health and Well-being

Healthcare systems globally face the problem of containing costs while trying to provide patient-centred services. SDG 3 aims at ensuring healthy lives and well-being for all. Both India and the Maldives have attempted to implement digital health policies, however, the laws in place do not tend to cater to the intricacies of digital health data. The DPDPA and Maldives' proposed Bill offer blanket data protection regulations; however, they fail to address the specificities of health data, including but not limited to the management of consent, data sharing policies, and the rights of patients in the digital sphere. This gap can restrict the optimal adoption of digital health technologies and, in turn, the fulfilment of SDG 3 (UN, n.d.-a).

Relevance to SDG 9: Industry, Innovation, and Infrastructure

Guided by the encompassing principles of sustain-

ability, SDG 9 aims to promote inclusive and sustainable industrialization alongside innovative practices. The legal frameworks in both countries offer a baseline for the protection of data; however, there are no available specific provisions that foster innovation within the field of digital health. For example, the lack of comprehensive policies on data sharing and interoperability may impede the creation of comprehensive digital health systems. In addition, the undefined policies on data sovereignty will stifle investment from the private health tech sector, consequently hindering the advancement toward SDG 9 (UN, n.d.-b).

Support for SDG 16: Peace, Justice, and Strong Institutions

SDG 16 aims to promote the peaceful and inclusive advancement of society, access to justice for all, and the creation of effective, responsible, and holistic institutions. The DPDPA and the Maldives' proposed Bill create data protection authorities responsible for ensuring compliance within the organization's set legal and regulatory framework on data protection. Authorities often face insufficient budgets, low levels of technical expertise, competing priorities, and political interference, which undermine the effectiveness of these authorities. Compounding this difficulty, the legal frameworks often grant broad exemptions to government agencies, which pose no transparency or accountability. These factors can whittle away public confidence in digital health systems and hinder the development of SDG 16 (UN, n.d.-c).

To align the governance frameworks with the SDGs, the gaps must be filled with explicit provisions dealing with legislative health data to remedy the governance framework.

These stages comprise formulating defined boundaries regarding consent, the anticipated activities of data utilization and expressions of patient interests, autonomy of the data protection agencies, and their capacity to execute their jurisdiction. This would enhance the digital healthcare ecosystems in India and the Maldives, thus strengthening contributions toward achieving the SDGs 3, 9, and 16.

RECOMMENDATIONS AND BEST PRACTICES

Both India and the Maldives must strike a balance within both interlinked frameworks for automated privacy, security, inclusivity, trust, healthcare data governance, and cross-border regulated health equity metrics. This paper puts forth curated recommendations and best practices aimed at enhancing the legal preparedness of both nations in advanced information management systems (Singh, 2024).

Unified Legal Frameworks

Embracing international frameworks. Both India and the Maldives need to overhaul their health data governance paradigms to comply with international law and transnational privacy regulations. Within the European Union, the European Health Data Space (EHDS) Regulation (EU) 2025/327, implemented in March 2025, serves as an advanced example, taking a holistic approach to data governance by ensuring patients' data access, portability, and interoperability with other member states. The Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System represents an alternative paradigm of privacy protection that facilitates transnational data flow.

Formulating a model law on health data governance. Transform Health, an international organisation, has developed a Model Law on Health Data Governance with core elements and legislative structures intended to improve domestic frameworks. The goal of the model law is to set a global standard for health-data legislation, creating harmonisation among states for cross-border data flows.

Multilateral and bilateral treaties. India and the Maldives should negotiate a bilateral Memorandum of Understanding (MOU) specifically governing cross-border health data transfer, given the volume of Maldivian patients seeking treatment in Indian hospitals. Such an MOU could define: (a) minimum security and consent standards for transmitting diagnostic records, prescriptions, and treatment histories between the two countries' healthcare systems; (b) a designated liaison mechanism between India's Data Protection Board and the Maldives' proposed Privacy Commissioner once the latter is operational; and (c) breach-notification timelines consistent with both DPDPA requirements and the Maldives' draft bill.

Defining 'trusted country' criteria under DPDPA Section 16. Section 16 of the DPDPA permits the Central Government to restrict transfers of personal data to specified countries or territories; however, it does not provide detailed criteria for determining such restrictions. India should therefore establish transparent criteria considering data-protection laws, regulatory capacity, security safeguards, data-subject rights, breach notification, and grievance-redress mechanisms. For the India-Maldives context, these criteria could be used to assess the Maldives once its data-protection framework and regulatory mechanisms become operational, an assessment that would promote secure and predictable cross-border health-data transfers while protecting patient privacy.

A phased adequacy standard for the Maldives. Given that the Maldives' Privacy and Personal Data Protection Bill remains in draft form, this paper proposes a phased approach: in the interim, health data transfers to India

could proceed under contractual safeguards modelled on standard contractual clauses, pending enactment; upon enactment of the bill and the operationalisation of the Privacy Commissioner, the Maldives could seek formal recognition as an adequate or trusted jurisdiction under DPDPA Section 16; and both countries could commit to periodic joint review of the arrangement as the Maldives' regulatory capacity matures.

Strengthening Institutional Capacities

Establishing independent data protection authorities. Both countries need to enhance or establish independent Data Protection Authorities (DPAs) whose function includes monitoring compliance in implementing laws that protect sensitive health information. These bodies must be allocated appropriate financial, technical, and legal resources commensurate with their enforcement capability to ensure compliance and remedial action.

Strategic capacity development programmes. There are definitive gaps that require directly tailored capacity development for healthcare practitioners, regulators, and policymakers. Such training should cover the protection of information, contemporary technologies, and ethics in health data, and should involve cooperation with international organisations for training and with academic institutions for resource mobilisation.

Forming unified national health data systems. Emphasis must be placed on systems that ensure security and interoperability in the exchange of information within the health sector. These include standardised frameworks for data and information, secure data storage, and controlled exchanges of information between health institutions. Such systems enhance the implementation of digital health initiatives by fortifying the integrity and confidentiality of data.

Improving Participation and Stakeholder Cooperation

Inclusive policy-making processes. The participation of consumers (patients), civil society, healthcare providers, information technology specialists, and other stakeholders is vital in policy formulation. This approach ensures that no pertinent issues are left unattended, thus enhancing the efficacy and equity of health data governance.

Awareness campaigns. Trust and participation in health initiatives can be achieved by educating the public about their rights related to health data, privacy, and e-health through awareness campaigns.

Feedback mechanisms. Many stakeholders are concerned about health data practices, and having robust feedback mechanisms allows for the reporting of issues

and the proposing of solutions. This approach is participatory and enhances transparency, accountability, and adaptability of health data governance.

CONCLUSION

The legal research on India and the Maldives had some significant achievements and issues for smart governance of health data. The Digital Personal Data Protection (DPDP) Act, 2023, has been a major step towards developing a more comprehensive and inclusive personal data protection law in India. The Act has a number of strong provisions governing the use of data, obtaining consent, and even cross-border data transfers, aiming to bolster privacy and security within the healthcare landscape.

The main concern has continued to be with the problems with protecting personal data, the measures taken to protect it (enforcement and compliance), and regulation rather than some more stringent methods.

Likewise, the proposed Privacy and Personal Data Protection Bill, 2023 is still in draft form, as of the time of writing, and has not been enacted into law, restricting the legal capacity of the country to govern digital health data. The Maldives lacks a comprehensive data protection law in place, as well as a data protection authority, unlike India which has DPDPA. The bill, if passed, will create a Privacy Commissioner instead of a dedicated Data Protection Authority. The Maldives also has a lack of infrastructure and a structural lack of skilled manpower for managing digitized health information. Despite the obstacles, both countries are on parallel paths towards digital transformation, with India having begun healthcare digital transformation initiatives like the Ayushman Bharat Digital Mission, and the Maldives having taken forward digital governance initiatives – such as its Digital Public Infrastructure – that create an enabling environment for health data systems while the dedicated legal framework is still to be enacted.

The study acknowledges its methodological shortcomings of using only the doctrinal approach. This is a powerful challenge to legal texts and policy frameworks, but not one that considers the lived experience of the patient or the healthcare provider and regulators. Empirical approaches to measuring the application of these laws in practice could be used in future research. This empirical knowledge could be used in conjunction with doctrinal research to gain a more comprehensive understanding of digital-health data governance.

Policy and Practice Implications

There is a need to create comprehensive smart health data regulations. It is essential that policymakers in India and the Maldives collaborate to develop effective data

protection policies that comply with international benchmarks set by agreements like the GDPR from the European Union. These policies would provide solutions for the appropriate and responsible management of sensitive health data.

The leaders in law and healthcare need to actively advocate for the creation of independent bodies with specific mandates to regulate data protection policies. Moreover, there is a critical gap in preparing the healthcare workforce, including providers and administrators, within the domain of continuous professional development, which equips them to govern health data in a worldwide digital context.

Future Research Directions

First, the evaluation of the DPDP Act together with the proposed Maldives Privacy and Personal Data Protection Bill needs to be subjected to a wider examination once the bill is passed. Empirical research on the implementation and effects of these schemes will improve the understanding of both legal systems and help to improve future policies.

Secondly, the need to develop cross-border exchange of digital health data is heavily highlighted, but it has to overcome significant obstacles such as compliance with multiple strands of legislation and regulations. When designing the legal and technical systems for the exchange of data, it is important that the necessary compliance with existing data protection laws is ensured.

Introspection of the countries that have developed more sophisticated digital health systems might help India and the Maldives to gain insights that they could adapt. The legal, technological, and cultural spaces that impact on the successful governance of smart health data should be explored in future studies.

To conclude, both India and the Maldives are making strides towards establishing relevant laws and regulations to govern and protect smart health data. But there is still a long way to go in the fight against obstacles and to achieve global standards. For a better tomorrow, both countries have to be more resilient to the challenges of the digital health age, the two countries could support each other with research, policy development and capacity building to ensure that health data is used to deliver better care and public health.

REFERENCES

- Alonso, C., Bhojwani, T., Hanedar, E., Prihardini, D., Uña, G., & Zhabaska, K. (2023). Stacking up the Benefits: Lessons from India's Digital Journey. <https://www.elibrary.imf.org/view/journals/001/2023/078/article-A001-en.xml>
- Bentotahewa, V., Hewage, C., & Williams, J. (2022). The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries. *SN Computer Science*, 3(3), 183. <https://doi.org/10.1007/s42979-022-01079-z>
- Countering Disinformation Effectively: An Evidence-Based Policy Guide. (2024). Carnegie Endowment for International Peace. Retrieved June 17, 2025, from <https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en>
- Crawford, G., & Lee, B. H. (n.d.). India's Digital Personal Data Protection Act 2023 vs. The GDPR: A Comparison. Latham Watkins. Retrieved <https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf>
- Cross-Border Data Transfer Requirements Under India DPDP Act. (2025). Securiti. Retrieved June 13, 2025, from <https://securiti.ai/cross-border-data-transfer-requirements-under-india-dpdp/>
- Data Protection Laws in India. (2025, January 6). DLA PIPER. <https://www.dlapiperdataprotection.com/?t=law&c=IN>
- Data protection laws in India—Data Protection Laws of the World. (2025). Retrieved June 13, 2025, from <https://www.dlapiperdataprotection.com/?t=law&c=IN>
- Davis, M. (2025). Understanding the Digital Personal Data Protection Act (DPDPA). OSANO. <https://www.osano.com/articles/digital-personal-data-protection-act-dpdp>
- Digital transformation: The Maldives' path to sustainable development and global leadership for SIDS | United Nations in Maldives. (2025). <https://maldives.un.org/en/291251-digital-transformation-maldives-path-sustainable-development-and-global-leadership-sids>
- Gaur, A. (2025). Cross-Border Data Flows and India's Digital Sovereignty. *Verfassungsblog*. <https://doi.org/10.59704/82a368a8a6158abf>
- Goh, J. J. K. (2024). Digital Health and Technology Adoption in Public Health. Retrieved June 13, 2025, from https://link.springer.com/rwe/10.1007/978-981-97-1788-0_32-1
- Group, G. L. (2025). International Comparative Legal Guides [Text]. Global Legal Group. (United Kingdom). International Comparative Legal Guides

- International Business Reports. Retrieved June 17, 2025, from <https://iclg.com/practice-areas/digital-health-laws-and-regulations/india>
- Holmgren, A. J., Esdar, M., Hüsters, J., & Coutinho-Almeida, J. (2023). Health Information Exchange: Understanding the Policy Landscape and Future of Data Interoperability. *Yearbook of Medical Informatics*, 32(1), 184–194. <https://doi.org/10.1055/s-0043-1768719>
- India Digital Personal Data Protection Act (DPDPA) 2023 Explained | Key Provisions & Impact. (2023). <https://secureprivacy.ai/>. Retrieved June 13, 2025, from <https://secureprivacy.ai/blog/india-digital-personal-data-protection-act-dpdpa-2023>
- Interoperability of privacy and data protection frameworks. (2021, December 22). OECD. <https://www.oecd.org/en/publications/interoperability-of-privacy-and-data-protection-frameworks/64923d53-en.html>
- Jayathissa, P., & Hewapathirana, R. (2023). Enhancing Interoperability among Health Information Systems in Low and Middle- Income Countries: A Review of Challenges and Strategies. *European Modern Studies Journal*, 7, 334–340. [https://doi.org/10.59573/emsj.7\(3\).2023.31](https://doi.org/10.59573/emsj.7(3).2023.31)
- Liang, L.-H. (2026, July 7). Maldives advances digital identity, digital transformation bills | Biometric Update. <https://www.biometricupdate.com/202607/maldives-advances-digital-identity-digital-transformation-bills>
- Maldives | Jurisdictions. (2023). DataGuidance. Retrieved June 17, 2025, from <https://www.dataguidance.com/jurisdictions/maldives>
- Maldives 2.0: President Launches Vision for a Digital-First Nation. (2025). Corporate Maldives. <https://corporatemaldives.com/maldives-2-0-president-launches-vision-for-a-digital-first-nation/>
- Maleki Varnosfaderani, S., & Forouzanfar, M. (2024). The Role of AI in Hospitals and Clinics: Transforming Healthcare in the 21st Century. *Bioengineering*, 11(4), 337. <https://doi.org/10.3390/bioengineering11040337>
- Mali, A. P. (2025). Consent under DPDPA - Comprehensive Understanding. Retrieved June 13, 2025, from <https://dpdpa.com/consentunderdpdpa.html>
- Mali, P. (2018). Privacy Law: Right to be Forgotten in India. *NLIU Law Review*, 7. <https://nliulawreview.nliu.ac.in/wp-content/uploads/2022/01/Volume-VII-17-33.pdf>
- Ministry of Electronics & IT. (2023, August 9). Salient Features of the Digital Personal Data Protection Bill, 2023. <https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=1947264>
- Ministry of Health and Family Welfare. (2021). A brief guide on Ayushman Bharat Digital Mission (ABDM) and its various building blocks. National Health Authority. https://abdm.gov.in:8081/uploads/ABDM_Building_Blocks_v8_3_External_Version_eabbc5c0f3_4_a96f40c645_5716a684de_b344369144.pdf
- Ministry of Health and Family Welfare. (2023). Annual Report 2022-23. National Health Authority. https://abdm.gov.in:8081/uploads/NHA_Annual_Report_2022_2023_4f3bc6e2a5.pdf
- PIB. (2015). Signing of a treaty between India and Maldives on Mutual Legal Assistance in criminal matters. <https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=129879>
- Qureshy, A. A., & Khan, S. (2024). Cross-Border Data Transfer Requirements Under India DPDPA. *Securiti*. Retrieved June 17, 2025, from <https://securiti.ai/cross-border-data-transfer-requirements-under-india-dpdpa/>
- Ramdas, K., Khuspe, K., Raut, A., Chavan, M., & Abhang, A. (2025). Comprehensive review on digital health innovations for improving rural healthcare delivery. *The Journal of Community Health Management*, 12, 3–13. <https://doi.org/10.18231/j.jchm.2025.002>
- Right to be Forgotten: Applicable against non-state entities? – Law School Policy Review. (2021). Retrieved June 13, 2025, from <https://lawschoolpolicyreview.com/2021/08/20/right-to-be-forgotten-applicable-against-non-state-entities/>
- Sarwal, R., Prasad, U., Gopal, K. M., Kalal, S., Kaur, D., Kumar, A., Regy, P., & Sharma, J. (2021). Investment Opportunities in India's Healthcare Sector. *Open Science Framework*. <https://osf.io/rtup2>
- Sharma, R. S., Rohatgi, A., Jain, S., & Singh, D. (2023). The Ayushman Bharat Digital Mission (ABDM): Making of India's Digital Health Story. *CSI Transactions on ICT*, 11(1), 3–9. <https://doi.org/10.1007/s40012-023-00375-0>
- Stevens, N. C., Philip. (2020). Building a Global Framework for Digital Health Services in the Era of COVID-19. <https://itif.org/publications/2020/05/26/building-global-framework-digital-health-services-era-covid-19/>
- UN. (n.d.-a). Health. United Nations Sustainable Development. Retrieved June 17, 2025, from <https://www.un.org/sustainabledevelopment/health/>
- UN. (n.d.-b). Infrastructure and Industrialization. United Nations Sustainable Development. Retrieved June 17, 2025, from <https://www.un.org/sustainabledevelopment/infrastructure-industrialization/>

UN. (n.d.-c). Peace, justice and strong institutions. United Nations Sustainable Development. Retrieved June 17, 2025, from <https://www.un.org/sustainabledevelopment/peace-justice/>

Understanding the Digital Personal Data Protection Act (DPDPA) 2023 | Tricog Health. (2024, November 29). <https://www.tricog.com/understanding-the-digital-personal-data-protection-act-dpdpa-2023/>

What is Data Protection Board under DPDP Law. (n.d.). Retrieved June 13, 2025, from <https://www.leegality.com/consent-blog/data-protection-board>

AUTHOR CONTRIBUTIONS

Author one conceptualised the study, developed the methodology, conducted the bibliographic retrieval and analysis, and contributed to the drafting and revision of the manuscript. Author two contributed to the interpretation of the Maldives-specific legal and policy context, validation of relevant local sources, and revision of the manuscript. Both authors reviewed and approved the final version of the manuscript and agree to be accountable for all aspects of the work.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support and academic environment provided by Mahindra University, Hyderabad, and Symbiosis International (Deemed University), Pune, which facilitated the completion of this research. The authors also acknowledge the scholarly contributions of the researchers and authors whose published literature, legal scholarship, and academic works that supported the development of this study.

DATA AVAILABILITY

The data used in this study are publicly available from the relevant bibliographic databases and scholarly and institutional sources.

FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

ETHICS APPROVAL

Ethics approval was not required because the study used publicly available bibliographic metadata and did not involve human participants, personal data collection, or intervention.

USE OF AI-ASSISTED TOOLS

Grammarly was used for grammar checking.