



# PDPA Compliance Challenges in Sri Lankan Cloud-Based Health Information Systems: A Qualitative Comparative Case Analysis of HHIMS, DHIS2, and Documentary Evidence

Y. P. Viduruwan\*<sup>id</sup>, M. G. P. Jeewantha<sup>id</sup>, M. A. P. Nimsara<sup>id</sup>,  
A. M. K. V. Abhayasundara<sup>id</sup>, K. M. Piyumal<sup>id</sup>  
University of Kelaniya, Sri Lanka

Received: June 9, 2026

Revised : August 17, 2026

Accepted : October 13, 2026

Online : October 14, 2026

## Abstract

In recent years, the country's digitisation efforts in health information systems have increased significantly, with the use of cloud-based systems integrated into both public and private health care networks. To meet the complex requirements of personal data protection, Sri Lanka's healthcare organisations dealing with sensitive patient data on cloud infrastructure must effectively navigate the new legal landscape established by the PDPA, which was enacted in 2022 and positions the country as the first in South Asia with holistic data protection laws. This paper conducts a case study that explores compliance issues of Cloud based Health Information Systems (HIS) in the context of PDPA in Sri Lanka. This study, based on a qualitative analysis of the provisions of the PDPA, a review of existing digital health deployments such as the Hospital Health Information Management System (HHIMS) and the District Health Information System (DHIS2) and a comparative analysis of international digital health protection frameworks like GDPR, HIPAA and ISO/IEC 27001, identifies six main compliance challenge domains: data localisation and cross-border transfer restrictions, consent management complexity, data protection officer (DPO) capacity gaps, cloud vendor accountability, breach notification readiness, and the ambiguity of PDPA's phased implementation. There are three main objectives discussed in this study: to identify the most relevant provisions of the PDPA for cloud-based processing of health data; to analyze the compliance gaps found in existing deployments of cloud-based health data in Sri Lanka; and to present a structured compliance framework, the PDPA-Aligned Cloud Health Compliance Framework (PACHCF), to help healthcare organizations meet these obligations. The paper then presents a proposed PDPA-Aligned Cloud Health Compliance Framework (PACHCF) to offer structured pathways for healthcare organisations. This study is an original and domain-specific compliance model in digital health governance that can be contextualized into Sri Lanka and South Asia. There isn't a peer-reviewed study that examines how the obligations in the PDPA relate to cloud-based health information systems in Sri Lanka (Data Protection Authority of Sri Lanka, 2023); nor any that sees governance, risk and compliance as an integrated issue in this context (Conduah et al., 2025). The study is designed for locations that have established organizations and existing technical systems. Sri Lanka does not have those systems at this time.

**Keywords:** *Personal Data Protection Act (PDPA), Cloud-Based Health Information Systems, Healthcare Data Governance, Data Localisation, Health Data Protection, Cross-Border Data Transfer, Digital Health Governance*

## INTRODUCTION

Digital technologies are reshaping the world of healthcare. Cloud computing, especially, has become a key part of present-day health information infrastructure, offering scalable, interoperable, and cost-effective data storage and processing for sensitive patient information (Armbrust et al., 2010). This shift in the digital revolution has strong potential to enhance service delivery, minimize administrative burden, and facilitate evidence-based health policy making in developing countries such as Sri Lanka (World Health Organization, 2021).

## Copyright Holder:

© Viduruwan, Leewantha, Nimsara, Abhayasundara & Piyumal. (2026)  
Corresponding author's email: [viduruw-cs20006@stu.kln.ac.lk](mailto:viduruw-cs20006@stu.kln.ac.lk)

## This Article is Licensed Under:



The national agenda for digital health is reflected in the national hospital health information management system (HHIMS), which has been implemented in 85+ government hospitals with over 9.5 million patients registered and about 23 million electronic medical records (EMR) maintained ([Information and Communication Technology Agency of Sri Lanka \[ICTA\], 2022](#)). In parallel, the Ministry of Health has implemented the District Health Information Software 2 (DHIS2) platform, which was quickly scaled up to support COVID-19 surveillance country-wide ([Exemplars in Global Health, 2021](#)). These deployments highlight the country's increasing use of cloud-based Health Information Systems (HIS) and the need for effective governance and security measures for patient data.

In this context, the introduction of the Personal Data Protection Act (PDPA) No. 9 of 2022 is a milestone in Sri Lanka's regulatory framework. Sri Lanka, the first South Asian country to enact a comprehensive data protection law ([Data Protection Authority of Sri Lanka, 2023](#)), has made it clear that it has a policy direction toward international privacy standards. The PDPA is largely modelled on the European Union's General Data Protection Regulation (GDPR) and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework ([Nithya Partners, 2022](#)), requiring authorities to adhere to principles of lawful processing, consent, data subject rights, breach notification, cross-border data transfers, and data protection officers (DPOs).

However, applying these obligations to cloud environments in healthcare creates additional complexity. The PDPA also considers health data to be a special category and therefore imposes stronger protections on the handling of such data ([Parliament of Sri Lanka, 2022](#)). While cloud architectures offer efficiency and scalability benefits, they also create inherent challenges, such as infrastructure being hosted by cloud service providers with data centres across multiple jurisdictions ([ISACA, 2024](#)). Additionally, the PDPA is subject to phased implementation, meaning that certain substantive aspects are not immediately in effect ([DLA Piper, 2025](#)), which has created uncertainty for healthcare organisations concerning their short-term compliance requirements.

This paper explores the PDPA compliance issues faced by cloud-based HIS in Sri Lanka through a qualitative case study. Three main objectives are outlined in the study: (i) to identify the most relevant provisions of the PDPA for cloud-based processing of health data; (ii) to analyse the compliance gaps found in existing deployments of cloud-based health data in Sri Lanka; and (iii) to present a structured compliance framework, the PDPA-Aligned Cloud Health Compliance Framework (PACHCF), to help healthcare organisations meet these obligations. The paper provides an original contribution by placing principles of governance, risk, and compliance in the context of a nationally situated and domain-specific compliance issue that has not yet been explored sufficiently in academic literature. There are two primary research questions addressed in this study. The first question is to examine how the principles of Governance, Risk, and Compliance relate to the technical architecture of healthcare platforms serving large populations. The second question is whether the study examines how organisations follow rules when the government is still in the process of changing the legal requirements.

## LITERATURE REVIEW

### Data Privacy Frameworks in Healthcare

Healthcare data repositories present high-value targets for malicious actors due to the concentration of sensitive personal and medical information ([Conduah et al., 2025](#)). This concentration of data can facilitate identity fraud, insurance fraud, and other forms of coercion. The Medical Ordinance of Sri Lanka, like most of the earlier health law, was concerned with the doctor-patient relationship ([Conduah et al., 2025](#)). Earlier data-protection practices were designed primarily around physical, paper-based records and did not anticipate the risks introduced by networked digital storage. The transition to electronic health records (EHRs) introduced novel

risks associated with distributed access, data sharing, and third-party processing risks that traditional medical ethics codes were not designed to address ([Rodrigues et al., 2013](#)).

The most common failure modes in digital systems are: sharing data with external parties, without adequate controls; granting access to too many people; honest mistakes made by staff, and retention policies that no one is following ([Conduah et al., 2025](#)). Maintaining comprehensive oversight of these failure modes requires substantial institutional resources. Requirements for security logs, identity verification of users may directly conflict with clinical reality, which is that a doctor needs a patient's history right away, rather than after having to go through three screens of security ([Rodrigues et al., 2013](#)).

### **GDPR as a Comparative Framework**

The General Data Protection Regulation (GDPR) is widely regarded as one of the most comprehensive data-protection frameworks currently in force. Article 9 of the GDPR classifies health, genetic, and biometric data as special categories of personal data for which processing is generally prohibited unless one of the specific conditions established under Article 9(2) applies, such as explicit consent or certain public-health, healthcare, or other legally defined grounds, an organization must have a defined legal basis for doing so, such as patient consent, public health need, or direct medical care ([European Parliament and Council, 2016](#)). The GDPR's extraterritorial scope applies to organizations that offer services to EU residents or monitor their behavior, regardless of where data processing occurs ([GDPR Local, 2025](#)).

The GDPR affords people real rights: to access their data, to correct it if it's incorrect, to delete it if they wish, and to move it elsewhere ([European Parliament and Council, 2016](#)). Data transfers outside of the EU may only occur after either European Commission authorization or a formal legal agreement to the recipient of the data. The reporting period to regulators runs for 72 hours if there is a breach that could cause harm to people. Implementation timelines for GDPR compliance may underestimate the practical resourcing and technical work required, particularly for organizations with legacy systems ([ComplianceHub, 2025](#); [Censinet, 2025c](#)).

The Sri Lankan Personal Data Protection Act (9/2022) is heavily based on the GDPR ([Parliament of Sri Lanka, 2022](#); [WilmerHale, 2022](#)). It puts data in people's hands, identifies some data types as being more sensitive and crucially mandates that privacy be considered from the outset in the design of systems. It is not possible to create an insecure structure and simply add in compliance at some later stage ([DLA Piper, 2025](#)).

### **ISO/IEC 27001 and HIPAA in Health Data Security**

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes privacy and security requirements specifically for protected health information (PHI) in the United States ([OneTrust, 2024](#)). It applies to healthcare organizations and their vendors, which need to sign Business Associate Agreements before handling any protected health information. HIPAA's Security Rule establishes administrative, physical, and technical safeguards for electronic protected health information, while the framework does not establish a general geographic data-localization requirement comparable to those found in certain other data-protection regimes. ([Kiteworks, 2026](#)).

ISO/IEC 27001 differs from the PDPA and GDPR in that it functions as a voluntary technical standard rather than a binding legal instrument. ISO/IEC 27001 is a voluntary, sector-agnostic standard that provides a structured framework for implementing and managing information security controls ([Censinet, 2025a](#)). The standard adopts a risk-based methodology requiring organizations to identify threats, select appropriate controls, and, if certification is sought, undergo independent third-party assessment. There is a companion standard, ISO/IEC 27701, that extends

the same framework, but to privacy specifically ([Censinet, 2025b](#)). Together, these frameworks provide guidance for implementing security controls such as encryption for data in transit and at rest and role-based access controls (RBAC) to restrict access to authorized personnel. In Sri Lanka, these standards provide a clear direction, not merely a legal requirement to interpret, for organizations seeking to fulfill PDPA requirements ([Scytale, 2025](#)).

### **Digital Health Governance in Sri Lanka**

Sri Lanka's formal digital health governance framework commenced in 2016 when the Ministry of Health, in collaboration with the Information and Communication Technology Agency (ICTA), published initial requirements for electronic health data management; In that year, the Ministry of Health besides ICTA published requirements for how organizations manage electronic health data ([Information and Communication Technology Agency of Sri Lanka \[ICTA\], 2021](#)). Because of this initial work, the National Digital Health Blueprint followed as a plan to store all health records from the country in one central system ([Ministry of Health, Nutrition and Indigenous Medicine Sri Lanka, 2023](#)). The interoperability architecture is based on OpenHIE standards, with HAPI-FHIR facilitating data exchange in a machine-readable format. HAPI-FHIR moves those records in a specific format that different computers are able to read ([Jayathissa & Hewapathrana, 2023](#)).

A distinctive feature of Sri Lanka's approach has been the parallel development of technical infrastructure and local human capacity. By working together, the Postgraduate Institute of Medicine, the University of Oslo or HISP Sri Lanka provide education for students in Biomedical Informatics ([Health Information Systems Programme \[HISP\] Sri Lanka, 2023](#)). To use the skills, individuals who finished those programs placed DHIS2 in clinics throughout the country ([Exemplars in Global Health, 2021](#)). On this platform they follow data about the health of mothers and children and they observe cases of tuberculosis. When the COVID-19 pandemic started, the individuals reacted in a short amount of time. For the response they created tools to monitor the spread of the disease ([Kinkade et al., 2022](#)). With the same goals, they made myHealth, which is a mobile application that allows people to see their personal health records.

### **Compliance Challenges in Emerging Data Protection Regimes**

Even in high-resource settings with established regulatory frameworks, data breaches remain prevalent. For example, HIPAA has been in force for nearly three decades, yet US healthcare organisations continue to experience significant breaches. It has been almost three decades since HIPAA became US law and data breaches in the gigantic healthcare industry still occur ([Conduah et al., 2025](#)). In 2017, WannaCry faulted major areas of the NHS thanks to the lack of patches for older systems ([Chatzou Dunford, 2026](#)). In the Singapore SingHealth breach, even well-resourced health systems are not spared ([ISACA, 2024](#)). In sub-Saharan Africa, structural constraints including limited trained personnel, weak enforcement mechanisms, and inadequate institutional capacity present persistent challenges to health information system implementation ([Mutale et al., 2013](#)).

The implementation gap between data-protection policy and organizational practice can be particularly challenging in developing-country contexts. A recurring pattern in developing country contexts is the treatment of privacy policies as compliance endpoints rather than foundational governance measures ([Numair et al., 2021](#)). There is no documentation of data flows within organizations. Records get stored on insecure servers or sent to offshore data centers that are not under the same data-processing agreement, if there is one but it's not enforced, or it is deemed invalid by law ([DPO Consulting, 2025](#)). Fundamental elements such as notification of a breach within 72 hours, consent controls, or the ability to collaborate with other public health institutions require institutional structures that are not always accessible to public health institutions ([ISACA,](#)

2024).

### **Theoretical Classification of Compliance Frameworks**

The compliance requirements examined in this study fall into three analytical categories: cross-sector statutory law, sector-specific legislation, and voluntary technical standards. The first category includes Sri Lanka's PDPA and the GDPR, which establish general obligations for collecting, processing, storing, and protecting personal data. The second includes HIPAA, which imposes additional privacy and security obligations specific to healthcare entities. The third includes ISO/IEC 27001, an international standard specifying requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).

These categories are complementary rather than interchangeable: statutory frameworks establish the legal obligations organisations must satisfy, while technical standards provide the practical mechanisms through which those obligations can be operationalised and monitored. For cloud-based health information systems, this distinction matters because compliance requires both legal accountability (who is responsible, under what law) and technical/organisational controls (how the obligation is actually met).

This theoretical classification is applied in Section 5 to systematically analyse the identified compliance issues and distinguish between legal-obligation gaps and technical-control gaps. The framework is applied to the evidence available in the reviewed documentation and therefore identifies potential compliance gaps rather than confirming operational deficiencies.

### **Novel Contribution**

In most academic studies regarding the governance of health data, researchers assume that the data exists within the General Data Protection Regulation or the Health Insurance Portability and Accountability Act (European Parliament and Council, 2016). There are frameworks in those regions that have existed for many decades. Because of this history, the regions have organizations with many financial resources to enforce laws and a large commercial sector for compliance. And while that research is useful, it is designed for locations that have established organizations and existing technical systems. Sri Lanka does not have those systems at this time. If an analyst applies the same findings to this country without changes, the results are not accurate.

The Personal Data Protection Act No. 9 of 2022 altered the way the government regulates privacy in Sri Lanka - but scholars have not published peer reviewed research on how this law applies to Health Information Systems that use cloud computing. To address this the current study operates from within the legal environment of Sri Lanka. It does not attempt to use foreign frameworks in a location for which they are not intended.

Building on the research questions outlined in Section 1, the contribution of this study is structured around three corresponding objectives: identifying the relevant provisions of the PDPA, analyzing potential compliance gaps in existing deployments, and developing a preliminary compliance framework.

The primary contribution of this study is the PDPA-Aligned Cloud Health Compliance Framework (PACHCF), which integrates PDPA obligations with cloud-specific technical and governance controls for public-sector health information systems. Based on the literature reviewed in this study, comparable integration of these legal, technical, and governance dimensions was not identified in the Sri Lankan digital health context. However, the framework has not yet undergone independent empirical validation and should therefore be regarded as a preliminary framework that provides a basis for further evaluation and refinement.

### Legal Interpretation of the PDPA for Cloud Environments

As stated in Section 10 of the PDPA, health data is a "special category" - because of this classification, the law requires more strict compliance than the rules for standard personal data. In this study the authors show how those obligations function when patient records exist on cloud infrastructure that is decentralized. To do this the study describes the necessary security settings and methods to minimize data. It also explains the legal risks that exist if the measures are not sufficient.

Although the PDPA is similar to the GDPR in its structure, the way that authorities enforce the law is different. When public health networks in a country send data through cloud providers in other countries, legal conflicts occur between different jurisdictions - those conflicts are not easy to solve using frameworks that people created for the EU. If a person applies those templates without changes, the results are often confusing rather than clear.

There is little guidance from peer reviewed sources that explains how PDPA rules apply to health systems that use the cloud. By conducting this study, the authors try to provide information where it is currently missing.

### Empirical Risk Assessment

In this article the authors describe a qualitative review of how two active national digital health platforms follow regulations. HHIMS contains 23 million electronic medical records that belong to 9.5 million citizens. DHIS2 is the platform that manages national disease surveillance. Both systems are essential when doctors make clinical decisions, when staff ensure patient safety and when institutions maintain accountability in Sri Lanka. For those reasons, the way the systems follow laws is a practical matter rather than a theoretical one.

There are six areas where problems occur regularly.

1. Under Section 26 of the PDPA, rules restrict where data is stored and how it moves across borders ([Parliament of Sri Lanka, 2022](#)).
2. It is difficult to manage how users give permission within public cloud architectures ([Nithya Partners, 2022](#); [Conduah et al., 2025](#)).
3. There is a lack of staff and resources to support the role of the Data Protection Officer ([DLA Piper, 2025](#); [Parliament of Sri Lanka, 2022](#)).
4. With multi-tenant contracts, it is difficult to hold cloud vendors accountable for security weaknesses ([Armbrust et al., 2010](#); [Censinet, 2025a](#)).
5. Due to a lack of preparation, gaps exist in how the organizations notify authorities about statutory breaches ([European Parliament and Council, 2016](#); [Kinkade et al., 2022](#)).
6. As the PDPA starts in stages, there is uncertainty regarding how the systems should operate ([WilmerHale, 2022](#); [Parliament of the Democratic Socialist Republic of Sri Lanka, 2025](#)).

## RESEARCH METHOD

### Research Design

This study adopts a qualitative, interpretivist case-study design. The case study method is suitable when the boundary between a phenomenon and its context is not clearly delineated ([Yin, 2018](#)), as the context itself is integral to the investigation rather than a peripheral factor ([Creswell & Creswell, 2018](#)). As this description matches the current research, PDPA compliance in cloud-based health systems occurs within Sri Lanka's specific regulatory structures, institutional constraints, and healthcare infrastructure. Treating these elements as separate from the system would render the analysis incomplete; they must be examined as interconnected components of the study.

### Case Selection

This study adopts a purposive sampling approach, selecting two primary systems that provide relevant cases for examining public-sector cloud-based health information systems in Sri Lanka. The two systems we examined were: (1) The Health System that is Managed by the Ministry of Health (MoH) from ICTA's perspective - known as the Health Information Management System (HHIMS), an electronic medical record system implemented at the hospital level and managed collaboratively by the Ministry of Health (MoH) and the Information and Communication Technology Agency (ICTA); and (2) District Health Information Software 2 (DHIS2) platform, a disease surveillance and health promotion system managed by the Ministry of Health (MoH).

These systems were selected based on three criteria: (a) they are implemented nationally across public health facilities; (b) they employ either fully-cloud based or a hybrid-cloud based architecture; (c) they manage patient health information, and (d) they have accessible technical and policy documentation ([Information and Communication Technology Agency of Sri Lanka, 2022](#); [Ministry of Health, Nutrition and Indigenous Medicine Sri Lanka, 2023](#)).

### Data Collection

The unit of analysis for this study comprises publicly available architectural blueprints, deployment reports, and policy documents relating to HHIMS and DHIS2. A systematic document search was conducted across academic databases (IEEE Xplore, ScienceDirect, PubMed) and institutional repositories (MoH, ICTA, WHO) between January and March 2026. Search strings utilised included: (*"cloud health systems" OR "health information systems"*) AND *"Sri Lanka"* AND (*"PDPA" OR "data protection"*).

The retrieved documents were initially screened by title and abstract, followed by full-text assessment of potentially relevant sources. Duplicate records and documents that did not provide information relevant to the architecture, governance, data management, or compliance characteristics of HHIMS or DHIS2 were excluded. The remaining documents were reviewed for evidence relating to data flows, storage arrangements, access controls, privacy mechanisms, governance responsibilities, and incident-management processes. Documents meeting the inclusion criteria were subsequently subjected to deductive and inductive thematic analysis.

### Data Analysis

Data were analyzed using the deductive and inductive thematic analysis approach outlined by Braun and Clarke ([Braun & Clarke, 2006](#)). A predefined codebook was established based on the statutory requirements of the PDPA (e.g., data localisation, consent management, breach notification, data subject rights, DPO responsibilities). Publicly available system capabilities were coded against these legal baselines to identify gaps. Inductive coding was subsequently applied to identify emergent patterns within each case, particularly regarding implementation challenges not explicitly addressed by the statutory framework.

Coding was performed by the primary researcher and reviewed by a supervisor to resolve ambiguities. Where disagreements occurred typically regarding the interpretation of technical documentation against legal requirements, they were resolved through discussion and consensus, with reference to the most recent official government or architectural documentation where conflicting evidence existed.

To ensure trustworthiness, credibility was supported through triangulation across multiple document types (legal texts, technical documentation, policy documents). Dependability was maintained through a consistent coding protocol applied across both cases. Reflexivity was addressed through explicit acknowledgment of the researcher's interpretive role in the absence of

direct organizational access (see Section 4.5).

Because this study relies on publicly available documentation rather than internal records, interviews, or audits, findings regarding organizational practice should be understood as inferences drawn from document evidence rather than confirmed operational states. Where the reviewed documentation did not describe a particular control or mechanism, this is reported as an absence from the available evidence rather than a confirmed absence in the operational system.

A compliance matrix was constructed to enable systematic comparison of PDPA obligations against other data protection regulations, including GDPR, HIPAA, and ISO/IEC 27001.

### **Research Limitations and Inferential Scope**

A significant constraint of this methodology is the reliance on publicly available documentation. Because the research team did not conduct internal institutional audits, stakeholder interviews, or technical penetration testing, the findings regarding organizational compliance are structural inferences drawn from public blueprints rather than confirmed operational states. Consequently, this study diagnoses potential compliance frictions based on documented system designs rather than internal day-to-day practices.

## **FINDINGS AND DISCUSSION**

### **Overview of PDPA Provisions Relevant to Cloud Health Systems**

The obligations of controllers and processors of personal data are set out in the PDPA No. 9 of 2022. There are a few provisions that are relevant to cloud-based health systems. Part II restricts processing of special category health data to instances where it is done with specific consent of the individual or in compliance with a statutory exception. Part III deals with data subject rights (access, rectification, erasure and objection) which must be executed in 21 business days of the request ([Parliament of Sri Lanka, 2022](#)). The enforcement and guidance body is established in Part V as the Data Protection Authority. The pace of implementation has been slow: Parts I, II, III, IV, and VII have been postponed numerous times in the Gazette, creating uncertainty regarding which provisions are currently in effect ([DLA Piper, 2025](#)).

The data localization rule for public authorities is the sharpest constraint for deployments in the cloud. Data must be processed within the boundaries of Sri Lanka, except where granted specific permission by the Data Protection Authority to process it offshore. Private sector organizations may share data with other jurisdictions only following an adequacy decision or with appropriate contractual safeguards ([Nithya Partners, 2022](#)). The challenge is that neither condition adequately fits the operational reality of major cloud providers, which store data by default across multiple data centers worldwide rather than by exception within a single jurisdiction.

### **Case Study Findings: Compliance Challenges**

Review of the HHIMS, DHIS2, and private sector cases identified six compliance challenge areas. The following analysis presents findings as inferences drawn from publicly available documentation rather than confirmed operational deficiencies. Where the reviewed documentation did not describe a particular control or mechanism, this is reported as an absence from the available evidence rather than a confirmed absence in the operational system.

#### *Challenge Domain 1: Data Localisation and Cross-Border Transfer Restrictions*

In local environments and on the Government Cloud (GCloud) of the ICTA, the HHIMS operates - but private hospitals use different systems, like AWS, Azure besides Google Cloud - those providers store data in multiple countries by default ([ISACA, 2024](#)). This practice does not align

with PDPA requirements for public authorities to keep data in specific locations. Similarly, private processors face challenges in meeting the adequacy or safeguard requirements for cross-border transfers, as the Minister has not issued a formal adequacy decision for any other country ([Parliament of Sri Lanka, 2022](#)).

The Cross Border Cloud Data Sovereignty framework from ISACA, there are four recommended actions - those actions are to record where data is at rest, verify compliance with local laws in each jurisdiction, investigate vendor backgrounds, and implement data masking and access limitation methods ([ISACA, 2024](#)). Based on a review of the current architectural documentation, there is no public evidence indicating that the health systems have fully implemented all four actions, suggesting limited documented readiness across the reviewed evidence.

#### *Challenge Domain 2: Consent Management Complexity*

Consent management in clinical settings presents inherent complexity. The PDPA requires consent to be specific, informed, voluntary, and revocable ([Parliament of Sri Lanka, 2022](#)). Sometimes in acute care, patients may be incapacitated, yet the Act doesn't explicitly address proxy consent. Interoperability between laboratory, pharmacy, e-Prescribing and radiology systems further complicates consent management. A patient may sign up at one point of care without realizing their data will be passed to integrated cloud systems for secondary processing ([Jayathissa & Hewapathrana, 2023](#)).

The concept of Data minimization, which requires processing to be limited, proportionate, and purpose specific, places additional stress on legacy health information architectures where clinical information is routinely passed to billing, management reporting and research, without any added layers of consent or purpose specification ([Conduah et al., 2025](#)).

The available HHIMS and DHIS2 documentation does **not describe** granular patient consent toggles or layered consent mechanisms. This absence suggests a potential gap between statutory requirements and documented system capabilities, though the possibility of undocumented features cannot be excluded.

#### *Challenge Domain 3: Data Protection Officer Capacity Gap*

The PDPA mandates that organizations that process special category data have a suitably qualified Data Protection Officer ([Parliament of Sri Lanka, 2022](#)). The role includes providing input on processing requirements, staff training, and privacy impact assessments. There are no publicly available documents identifying dedicated DPO appointments within Sri Lanka's public health HIS deployments. The Data Protection Authority, established in 2023, has not yet published DPO qualification standards or a practitioners register ([DLA Piper, 2025](#)). Healthcare organizations face uncertainty in filling a position for which no official definition of required qualifications exists. This challenge is compounded by the limited pool of information security professionals in Sri Lankan healthcare ([HISP Sri Lanka, 2023](#)).

#### *Challenge Domain 4: Cloud Vendor Accountability and Contractual Controls*

The PDPA imposes a duty on controllers to oversee processor data processing and requires binding data processing agreements with processors ([Parliament of Sri Lanka, 2022](#)). Typical contracts offered by international cloud service providers do not generally provide PDPA obligations regarding rights of the data subject, notification schedules or audits. Large vendors hold stronger negotiating positions, making bespoke agreements difficult to obtain ([Censinet, 2025a](#)). Sub-processing (subcontracting work to another provider) adds accountability layers that are difficult to trace. Existing literature highlights the importance of security certifications, such as

ISO/IEC 27001, when evaluating healthcare cloud service providers, alongside appropriate contractual safeguards (Rodrigues et al., 2013). However, the publicly available documentation reviewed in this study does not establish whether such requirements are consistently incorporated into the standard cloud-service arrangements used by Sri Lanka's public healthcare sector for deployments such as HHIMS and DHIS2.

#### *Challenge Domain 5: Breach Notification Readiness*

Under the PDPA, a controller is required to inform the Data Protection Authority after a data breach occurs. The Authority determines when and how notification occurs. As of the time of this study, no official rules for notifications have been released. Healthcare organisations are therefore uncertain about the specific steps they must take.

For context, the GDPR requires notification within 72 hours, with proposed 2025 plans potentially reducing this to 48 hours for the health industry (ComplianceHub, 2025). HIPAA allows 60 days for breaches affecting more than 500 individuals (OneTrust, 2024). At present, no publicly available documentation identified for HHIMS, DHIS2, or comparable Sri Lankan HIS deployments describes automated breach detection or notification features. This absence from the reviewed evidence should not be read as confirmation that no such deployment has these features.

#### *Challenge Domain 6: Phased Implementation Ambiguity*

The Personal Data Protection Act became effective through a gradual process that results in a regulatory challenge within Sri Lanka. By the Amendment Act No. 22 of 2025, the government deleted the sections that allowed for a delay in enforcement (Parliament of the Democratic Socialist Republic of Sri Lanka, 2025). While this made the primary requirements of the law active, the Data Protection Authority has not provided industry-specific guidance. Healthcare organisations are aware the law is active but lack information about how they must comply in their specific field. This situation is consistent with findings from other studies on data laws in South and Southeast Asia, which document the delay that often exists between enactment and full operability (Numair et al., 2021; Mutale et al., 2013).

### **Proposed Framework: PDPA-Aligned Cloud Health Compliance Framework (PACHCF)**

In light of the results of the case study analysis, comparative regulatory analysis and the literature on governance, this paper introduces the PDPA-Aligned Cloud Health Compliance Framework (PACHCF). The framework is organized into seven governance domains, each addressing one or more of the identified compliance issues. The PACHCF is intended to be applicable to any public or private healthcare provider implementing cloud based HIS in Sri Lanka.

**Table 1.** PDPA-Aligned Cloud Health Compliance Framework (PACHCF)

| Domain                                                               | What It Does                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Domain 1<br/>Statutory Compliance &amp;<br/>Data Localisation</b> | Grounded in Sections 10 (special category health data) and Section 26 (geographical restrictions on public authority data), which together establish the minimum compliance threshold. This involves identifying the data, ensuring public authority health data stays within Sri Lanka, subject to exception granted by the Data Protection Authority (DPA), and ensuring the adequacy or sufficient safeguards are in place for any transfer of private data across borders. |
| <b>Domain 2<br/>Consent &amp; Data Subject</b>                       | Governs the lawful processing of data. Consent for health data must be clear and revocable, with proxy consent mechanisms                                                                                                                                                                                                                                                                                                                                                      |

| Domain                                                                           | What It Does                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rights Management</b>                                                         | available where personal consent cannot be obtained. Layered consent is the act of informing the data subject of the data being collected at a certain time being used for a different purpose. There are parallel processes for the exercise of these subject data rights: the right to access, the right to rectification, the right to erasure, and the right to objection.                                                                                                                                                                                                                                                                              |
| <b>Domain 3<br/>Data Protection Officer Capacity</b>                             | The focus of this domain is on the Data Protection Officer. The position should be filled with a true compliance professional who can recommend processing decisions, conduct privacy impact assessments, and increase employee awareness. It also involves structured training and internal capacity building due to the lack of individuals who can adequately perform the role in Sri Lanka. When there is no in-house expertise, shared or outsourced Data Protection Officer arrangements are viable solutions whilst the formal standards for the qualification of a DPO are agreed by the Data Protection Authority.                                 |
| <b>Domain 4<br/>Cloud Vendor Accountability &amp; Contractual Controls</b>       | Cloud contracts require tailored Data Processing Agreements that eliminate cross-border sub-processing and mandate that vendors conform to breach-notification deadlines required in their local countries. The due diligence process must be extended through the sub-processing tier; vendors certified to ISO/IEC 27001 or equivalent standards are preferred where organizational maturity allows.                                                                                                                                                                                                                                                      |
| <b>Domain 5<br/>Breach Notification &amp; Incident Response Readiness</b>        | This sets up a formal incident response plan. Sri Lanka's own rules are still to be finalised, but there are two benchmarks to follow: the GDPR's 72-hour notification window and HIPAA's large-break notification window. The technical aspects of this domain convert compliance requirements to engineering requirements, such as the creation of zero-trust access control, end-to-end encryption and immutable audit logs, translating them into controls in ISO/IEC 27001 Annex A. Implementations are auditable in terms of compliance, with AI-assisted breach detection as a future enhancement once foundational monitoring capacity is in place. |
| <b>Domain 6<br/>Regulatory Monitoring &amp; Phased-Implementation Adaptation</b> | The PDPA's implementation has been a gradual process, and the phase-out of all grace-period provisions in Amendment Act No. 22 of 2025 has left companies facing uncertainty regarding compliance. Organisations must constantly be alert for Gazette notifications, and have a scheduled compliance path prioritised allowing training, technology and processes to continue while awaiting sector-specific timelines from the Data Protection Authority.                                                                                                                                                                                                  |
| <b>Domain 7<br/>Health Data Governance Committee</b>                             | Establishes a standing Health Data Governance Committee to take over compliance as a continuous effort, not a single solution. The committee also oversees the other six domains and conducts regular Privacy Impact Assessments, reviews policy and serves as the institutional foundation for automated monitoring and                                                                                                                                                                                                                                                                                                                                    |

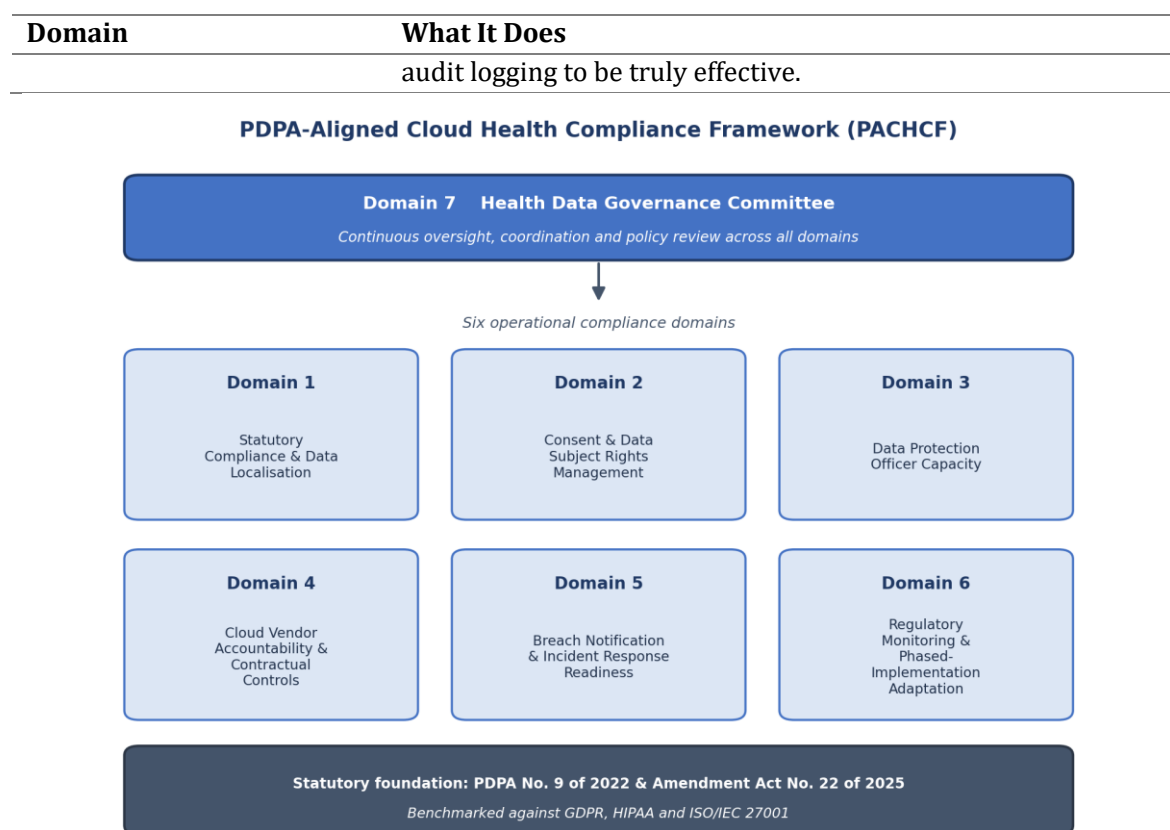


**Figure 1.** The seven governance domains of the PDPA-Aligned Cloud Health Compliance Framework (PACHCF)

### Derivation of Domain 7

The first six domains were derived from compliance issues identified during the document analysis of HHIMS and DHIS2. The seventh domain, Health Data Governance Committee, differs in that it represents a proposed governance mechanism rather than an empirically observed feature of either system. It was introduced to address the coordination gap between legal requirements, information-security controls, system administrators, healthcare institutions, and cloud service providers, drawing on governance literature (Mutale et al., 2013; Yin, 2018) on continuous compliance. It should therefore be interpreted as a design recommendation informed by the analysis, rather than a finding directly established by case evidence.

### Comparative Analysis: PDPA vs. International Frameworks

**Table 2.** Comparative Analysis: PDPA vs. International Frameworks

| Compliance Vector                 | Sri Lanka PDPA                                                                               | EU GDPR                                                                                                        | US HIPAA                                                                              | ISO/IEC 27001                                                       |
|-----------------------------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| <b>Health Data Classification</b> | Special Category (Section 10) requires explicit consent or a recognized statutory exemption. | Special Category (Article 9) processing prohibited except under explicit public health or research exemptions. | Protected Health Information (PHI) governed by integrated Privacy and Security Rules. | Classified under asset management and risk categorization controls. |

| <b>Compliance Vector</b>                          | <b>Sri Lanka PDPA</b>                                                                                                               | <b>EU GDPR</b>                                                                                                          | <b>US HIPAA</b>                                                                  | <b>ISO/IEC 27001</b>                                                                       |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <b>Data Localisation &amp; Cross-Border Flows</b> | Absolute localisation for public authorities (Section 26) data must stay in Sri Lanka unless the DPA grants explicit authorization. | No absolute localization relies on adequacy decisions, standard contractual clauses (SCCs), or binding corporate rules. | No geographic restrictions rely on encryption and Business Associate Agreements. | Control A.8.24 (Cryptography) and network segregation protect distributed cloud pipelines. |
| <b>Breach Notification Timelines</b>              | Reporting to the DPA requires specific windows still being defined under the phased enforcement schedule.                           | 72-hour window to notify the supervisory authority after becoming aware of a breach.                                    | Up to 60 days for large-scale breaches affecting more than 500 individuals.      | Requires structured incident response policies to capture and document security events.    |
| <b>Cloud Governance &amp; Vendor Liability</b>    | Joint and several liability for controllers and processors is a legally binding data processing terms required.                     | Formal distinction between Controller and Processor data processing contracts mandatory.                                | Direct statutory liability for cloud vendors via Business Associate Agreements.  | Control A.5.23 (Cloud Services Security) mandates supply-chain risk management.            |

## Discussion

In this analysis, the six domains of compliance challenges are connected rather than separate. They increase the difficulty of one another and the impact is most significant for private providers with few employees and public health facilities in rural areas (Numair et al., 2021). Institutional capacity is already low in those locations (Conduah et al., 2025).

Due to the lack of clarity regarding how to implement stages in Domain 6, the other domains are more difficult to address. When the regulator does not provide specific instructions about schedules or requirements for the health sector, organizations cannot decide with certainty which tasks are important or how much resource to allocate. If the Data Protection Authority provides specific guidance similar to the documents the UK Information Commissioner's Office created for GDPR (Conduah et al., 2025), organizations will have a clear basis for their actions - this support is likely to increase the speed at which entities adopt the required standards.

The findings suggest that improving compliance should not be approached solely as a matter of introducing additional security technologies. Greater attention is also required at the governance and operational level, for example, by establishing clearer data-protection responsibilities, documenting data flows between HIS components and cloud services, and periodically reviewing third-party processing arrangements against PDPA requirements. Technical measures such as stronger identity controls, continuous monitoring, and zero-trust principles can then support these governance measures rather than operate independently of them (Rodrigues et al., 2013).

To address the vulnerabilities identified in the breach readiness and vendor accountability

domains, healthcare organizations may consider integrating advanced technical controls as they mature. For instance, the deployment of Zero-Trust Architectures (ZTA) and AI-assisted breach monitoring could provide automated telemetry currently not documented in Sri Lanka's HIS (Rodrigues et al., 2013). While resource-intensive, exploring tamper-evident audit mechanisms and distributed ledger approaches for consent and access auditing has been identified in recent literature as a potential mechanism for satisfying stringent data immutability requirements (Conduah et al., 2025). Their adoption should, however, be evaluated against practical considerations including scalability, interoperability, privacy, governance, and implementation cost.

Where internal capacity is lacking, organisations should explore outsourced or shared DPO arrangements to meet statutory mandates without straining individual hospital budgets. As the Data Protection Authority has not yet published formal qualification standards, interim arrangements can be structured to ensure continuity while formal guidance is developed.

As a framework, the PACHCF is not a simple checklist. In Domain 7, the Health Data Governance Committee exists so that the act of following regulations is a permanent organisational activity rather than a reaction to specific issues. As academic sources indicate, individual evaluations are insufficient because the process of meeting data protection standards is continuous (Mutale et al., 2013; Yin, 2018).

## CONCLUSIONS

In this paper, we have introduced a systematic case study analysis of the compliance issue for the application of Sri Lanka's Personal Data Protection Act No. 9 of 2022 to Health Information Systems (HIS) in the cloud. In the context of the national health platforms (HHIMS and DHIS2), comparative analysis to GDPR, HIPAA and ISO/IEC 27001, and a comprehensive literature review, six main compliance challenge domains were identified: Data Localisation and Cross-border Transfer Restrictions, Consent Management Complexity, DPO capacity gaps, Cloud Vendor Accountability, Breach Notification Readiness, and Phased Implementation Ambiguity. The first objective was addressed through a legal and regulatory interpretation of the PDPA provisions relevant to cloud-based health information systems. The analysis indicates that health data, as a special category of personal data, creates heightened compliance requirements concerning lawful processing, consent, data-subject rights, data localization and cross-border transfers, Data Protection Officer responsibilities, processor accountability, and breach notification.

The second objective was addressed by examining documentary evidence relating principally to HHIMS and DHIS2 and comparing the identified issues across the selected cases and relevant international frameworks. The third objective was to develop a structured framework that connects the identified compliance challenges with potential governance responses. The resulting PDPA-Aligned Cloud Health Compliance Framework (PACHCF) organizes the issues into seven proposed governance domains: statutory compliance and data localization; consent and data-subject rights management; Data Protection Officer capacity; cloud vendor accountability and contractual controls; breach notification and incident-response readiness; regulatory monitoring and phased-implementation adaptation; and a Health Data Governance Committee.

To address these challenges, the paper introduces the PDPA-Aligned Cloud Health Compliance Framework (PACHCF), a seven-domain governance model to offer healthcare organisations suitable actionable compliance pathways based on the PDPA obligations and guided by international standards. The PACHCF is an original piece of GRC scholarship and a valuable addition to the literature of practice in how to govern the digital health space in Sri Lanka.

The results have a number of implications for policies and practice. The DPA SL should focus on providing guidelines on data protection for the healthcare sector, qualification standards

for DPOs, and a streamlined process to notify the breach. The requirements of PDPA should be incorporated into the implementation planning of the Digital Health Blueprint by the Ministry of Health, including requirements for DPIA for new deployments of HIS. Healthcare organisations can implement ISO/IEC 27001 as a baseline compliance framework, set up Health Data Governance Committees and negotiate PDPA compliant agreements with cloud service providers.

### LIMITATION & FURTHER RESEARCH

There are some limitations to this study. It is a qualitative case study, so the results cannot be statistically generalised to other cases (Yin, 2018). but the analytical generalisability of the PACHCF framework goes beyond the specific cases studied (Creswell & Creswell, 2018). In the majority of instances, the study has been based on data found in publicly available documents and the internal compliance files of healthcare organisations were not acquired. Also, the framework of the PDPA is ongoing and subsequent announcements or guidance of the Data Protection Authority may impact the compliance picture since the publication of this paper. The study did not include primary data collection through interviews or observations. In particular, perspectives from Data Protection Officers (DPOs), system administrators, health information managers, cloud service personnel, legal practitioners, and other relevant stakeholders were not directly solicited. The legal interpretation presented in the study has not been independently validated by legal or data-protection experts. The analysis interprets the PDPA in relation to cloud-based health information systems and compares selected requirements with the GDPR, HIPAA, and ISO/IEC 27001.

This qualitative study should be continued by quantitative surveys of the extent to which the healthcare industry in Sri Lanka is prepared for PDPA, empirical analysis of the effectiveness of implementation of the PACHCF and the developments in regulations over a period of time as more guidance is issued by the Data Protection Authority. Further, research directions that investigate the use of privacy-enhancing technologies like federated learning and differential privacy in Sri Lankan health data ecosystems also open new avenues for building on these contributions.

### REFERENCES

- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50–58. <https://doi.org/10.1145/1721654.1721672>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp0630a>
- Censinet. (2025a). *GDPR vs. HIPAA: Cross-border breach rules*. <https://censinet.com/perspectives/gdpr-vs-hipaa-cross-border-breach-rules>
- Censinet. (2025b, December 24). *How ISO 27001 secures patient data*. <https://censinet.com/perspectives/how-iso-27001-secures-patient-data>
- Censinet. (2025c). *ISO 27001 vs. HIPAA: Compliance in healthcare*. <https://censinet.com/perspectives/iso-27001-vs-hipaa-compliance-healthcare>
- Chatzou Dunford, M. (2026, April 30). *Healthcare data sovereignty compliance: What it means and why it matters for your organization*. Lifebit. <https://lifebit.ai/blog/healthcare-data-sovereignty-compliance/>
- ComplianceHub. (2025). *GDPR 2025 updates: Navigating cross-border transfers and stricter breach reporting*. <https://compliancehub.wiki/gdpr-2025-updates-navigating-cross-border-transfers-and-stricter-breach-reporting/>
- Conduah, A. K., Ofoe, S., & Siaw-Marfo, D. (2025). Data privacy in healthcare: Global challenges and solutions. *Digital Health*. <https://doi.org/10.1177/20552076251343959>
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods*

- approaches* (5th ed.). SAGE Publications.
- Data Protection Authority of Sri Lanka. (2023). *About the PDPA*. <https://www.dpa.gov.lk/>
- DLA Piper. (2025). *Data protection laws of the world: Sri Lanka*. <https://www.dlapiperdataprotection.com/index.html?t=law&c=LK>
- DPO Consulting. (2025, December 5). *Cross-border data transfers: A global guide to compliance*. <https://www.dpo-consulting.com/blog/cross-border-data-transfers>
- European Parliament and Council. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Official Journal of the European Union.
- Exemplars in Global Health. (2021). *DHIS2 in Sri Lanka*. <https://www.exemplars.health/emerging-topics/epidemic-preparedness-and-response/digital-health-tools/sri-lanka>
- GDPR Local. (2025). *Digital sovereignty: Data control and compliance in a digital world*. <https://gdprlocal.com/digital-sovereignty/>
- Health Information Systems Programme Sri Lanka. (2023). *Digital health capacity building*. Postgraduate Institute of Medicine, University of Colombo.
- Information and Communication Technology Agency of Sri Lanka. (2021). *Outcome assessment of the Digital Health Project: Hospital Health Information Management System (HHIMS) final report*. <https://www.icta.lk/icta-assets/uploads/2023/02/Digital-Health-Project-HHIMS-Final-Report-V-1-13th-July-2021-1.pdf>
- Information and Communication Technology Agency of Sri Lanka. (2022). *Hospital health information management system (HHIMS)*. <https://www.icta.lk/projects/digital-government/hospital-health-information-management-system-hhims>
- ISACA. (2024). *Cloud data sovereignty, governance and risk implications of cross-border cloud storage*. <https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage>
- Jayathissa, P., & Hewapathrana, R. (2023). HAPI-FHIR server implementation to enhancing interoperability among primary care health information systems in Sri Lanka: Review of the technical use case. *European Modern Studies Journal*, 7(6), Article 23. [https://doi.org/10.59573/emsj.7\(6\).2023.23](https://doi.org/10.59573/emsj.7(6).2023.23)
- Kinkade, C., Russpatrick, S., Potter, R., Saebo, J., Sloan, M., Odongo, G., Singh, T., & Gallagher, K. (2022). Extending and strengthening routine DHIS2 surveillance systems for COVID-19 responses in Sierra Leone, Sri Lanka, and Uganda. *Emerging Infectious Diseases*, 28(13), Article 22-0711. <https://doi.org/10.3201/eid2813.220711>
- Kiteworks. (2026). *Healthcare data sovereignty: Requirements for transferring patient data across borders*. <https://www.kiteworks.com/hipaa-compliance/healthcare-data-sovereignty-cross-border-transfer/>
- Ministry of Health, Nutrition and Indigenous Medicine Sri Lanka. (2023). *Digital health blueprint*. OpenHIE. [https://ohie.org/wp-content/uploads/2024/04/DigitalHealthBluePrint\\_SRILANKA-2.pdf](https://ohie.org/wp-content/uploads/2024/04/DigitalHealthBluePrint_SRILANKA-2.pdf)
- Mutale, W., Chintu, N., Amoroso, C., Awoonor-Williams, K., Phillips, J., Jackson, E., Taylor, A., Schwarz, R., Faye Iarrobino, M., & Sherr, K. (2013). Improving health information systems for decision making across five sub-Saharan African countries: Implementation strategies from the African Health Initiative. *BMC Health Services Research*, 13(Suppl. 2), Article S9. <https://doi.org/10.1186/1472-6963-13-S2-S9>
- Nithya Partners. (2022). *Data protection legislation in Sri Lanka*. <https://www.nithyapartners.com/journal/data-protection-legislation-in-sri-lanka>
- Numair, T., Harrell, D. T., Huy, N. T., Nishimoto, F., Muthiani, Y., Nzou, S. M., Lasaphonh, A., Palama, K., Pongvongsa, T., Moji, K., Hirayama, K., & Kaneko, S. (2021). Barriers to the digitization of health information: A qualitative and quantitative study in Kenya and Lao PDR using a

- cloud-based maternal and child registration system. *International Journal of Environmental Research and Public Health*, 18(12), Article 6196. <https://doi.org/10.3390/ijerph18126196>
- OneTrust. (2024). *HIPAA vs. ISO 27001: What's the difference?* <https://www.onetrust.com/blog/hipaa-vs-iso-27001-whats-the-difference/>
- Parliament of Sri Lanka. (2022). *Personal Data Protection Act, No. 9 of 2022 (Sections 5–43)*. Government of Sri Lanka. <https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf>
- Parliament of the Democratic Socialist Republic of Sri Lanka. (2025). *Personal Data Protection (Amendment) Act, No. 22 of 2025*. <https://www.parliament.lk/uploads/acts/gbills/english/6384.pdf>
- Rodrigues, J. J. P. C., De La Torre, I., Fernández, G., & López-Coronado, M. (2013). Analysis of the security and privacy requirements of cloud-based electronic health records systems. *Journal of Medical Internet Research*, 15(8), Article e186. <https://doi.org/10.2196/jmir.2494>
- Scytale. (2025). *HIPAA vs. ISO 27001: What's the difference?* <https://scytale.ai/resources/hipaa-vs-iso-27001/>
- WilmerHale. (2022, March 30). *Sri Lanka becomes the first South Asian country to pass comprehensive privacy legislation*. <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20220330-sri-lanka-becomes-the-first-south-asian-country-to-pass-comprehensive-privacy-legislation>
- World Health Organization. (2021). *Digital health*. <https://www.who.int/health-topics/digital-health>
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.