Trends in Health Informatics

www.thi.reapress.com

THI. Vol. 3, No. 1 (2026) 51–73.

Paper Type: Original Article

Privacy and Data Security in Medical Tourism: A Systematic Review of Health Information Exchange Risks, Legal and Regulatory Challenges, and Technology-Based Solutions

Esmail Shabnani Nejad[1,*], Nastaran Laleh[2]

[1] Department of Management, University of Tehran, Tehran, Iran; Esmail.shabani@ut.ac.ir.
[2] Department of Tourism, University of Mazyar, Royan, Iran; nastaran.l68@gmail.com.

Citation:

Received: 07 May 2025 *Revised: 23 August 2025* *Accepted: 04 October 2025*	Shabnani Nejad, E., & Laleh, N. (2026). Privacy and data security in medical tourism: A systematic review of health information exchange risks, legal and regulatory challenges, and technology-based solutions. *Trends in Health Informatics, 3*(1), 51-73.

Abstract

Medical tourism, a rapidly expanding industry with an annual market value exceeding $400 billion, has developed on an inadequate foundation of health data protection infrastructure. The cross-border exchange of clinical information exposes patient privacy to multiple security and regulatory risks that remain inadequately addressed. This systematic review aimed to identify and analyze security and privacy risks, legal and regulatory challenges, and technology-based solutions for protecting health data in medical tourism contexts. A systematic review following Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines was conducted through systematic searches across five major databases, Scopus, Web of Science, PubMed, ScienceDirect, and Google Scholar, for peer-reviewed articles published between 2015 and 2025. Inclusion criteria encompassed peer-reviewed English-language studies addressing medical tourism, health data security, and protective technologies. Of 1,247 articles initially identified, 52 studies were selected for analysis. Two independent reviewers conducted quality assessments using thematic analysis to extract relevant data. The findings revealed that the most prevalent security risks included data breaches (80.8% of studies), unauthorized access (73.1%), and cyberattacks (78.8%), with average breach costs ranging from $408,000 to $600,000 per incident. Major legal and regulatory challenges identified included heterogeneous data protection laws across jurisdictions (92.3% of studies), undefined jurisdictional authority (80.8%), restricted cross-border data transfer (84.6%), and inadequate informed consent procedures (75.0%). Identified technology-based solutions encompassed advanced encryption (67.3%), Artificial Intelligence (AI) (42.3%), secure cloud computing (48.1%), blockchain (34.6%), digital identity management (36.5%), and Zero Trust architecture (26.9%). However, no single technology provides a complete solution; effective implementation requires an integrated combination of technological, organizational, and legal measures. This review demonstrates that protecting privacy and security of health data in medical tourism represents a multidimensional challenge requiring a comprehensive and balanced approach. Narrowing international legal gaps, enhancing patient consent procedures, and establishing coordinated agreements are essential for building trust and ensuring industry sustainability.

Keywords: Medical tourism, Data privacy, Cross-border health information exchange, Legal and regulatory challenges, Emerging technologies.

1 | Introduction

Medical tourism, recognized as one of the fastest-growing sectors in the global economy, encompasses the cross-border movement of individuals seeking healthcare services in countries other than their country of

Corresponding Author: Esmail.shabani@ut.ac.ir
https://doi.org/10.22105/thi.v3i1.46

residence, and has undergone remarkable expansion over the past two decades. According to reports from the World Tourism Organization, the global number of medical tourists increased from approximately 100 million in 2000 to over 200 million in 2020 [1], [2]. This rapid growth extends beyond economic factors and cost reduction in healthcare delivery; rather, it reflects the pursuit of improved access to advanced medical services, reduced waiting times for elective procedures, and access to specialized treatments [3]. Current projections indicate that this sector comprises approximately 2.5% to 3% of the global tourism market and is expected to achieve annual growth rates of approximately 15% through 2030 [4]. The economic significance of medical tourism for participating nations is substantial, as many developing countries leverage this industry to generate foreign currency revenue and create employment opportunities.

The proliferation of digital technologies has fundamentally transformed medical tourism through the digitalization of health information and its exchange among healthcare facilities and across national borders. Electronic Health Records (EHR) systems, combined with telemedicine services and digital health platforms, have enabled patients and clinicians to access comprehensive medical histories and diagnostic details instantaneously [5]. Cloud-based implementations of these systems have further facilitated the sharing of health information among healthcare providers located in different countries. Cross-border Health Information Exchange (HIE), while offering substantial potential benefits for improving clinical outcomes and accelerating diagnostic processes, presents multifaceted technical and legal challenges that have received insufficient research attention [6].

Health information, encompassing medical histories, laboratory results, diagnostic imaging, and genetic data, constitutes one of the most sensitive and personally identifiable categories of individual data. In contrast to other sensitive data types, the misuse of health information can precipitate serious consequences for individuals in economic, social, and psychological domains. Potential harms include employment discrimination, insurance denial, physical injury, and psychological distress [7]. Consequently, privacy protection and security assurance of health information represent not only legal and regulatory imperatives but also ethical principles essential for maintaining patient trust in healthcare systems. The escalation of cybercriminal activity and digitalization-related vulnerabilities have intensified concerns regarding health information security to unprecedented levels.

Contemporary healthcare environments are confronted with an increasingly diverse and sophisticated array of security threats. Health data breaches represent one of the most prevalent and consequential threats facing patients and healthcare organizations alike; surveillance data indicate that health sector breaches have increased by more than 50% over the past five years [8]. Unauthorized access, a range of cyberattacks, including ransomware, phishing, and Distributed Denial-of-Service (DDoS) attacks, and identity theft collectively constitute major threats to health information security. These external threats are further compounded by internal system vulnerabilities within HIE platforms [8]. In the medical tourism context, these risks are substantially amplified by the involvement of multiple governments, institutions, and technology systems operating under divergent standards. Interoperability deficiencies, inadequate standardization, and cross-border data transfer pathways create conditions that are particularly conducive to security breaches and systemic vulnerabilities [9].

Legal and regulatory challenges in cross-border HIE represent among the most complex dimensions of this issue. Data protection and privacy regulations vary considerably across jurisdictions in stringency and scope. The General Data Protection Regulation (GDPR) of the European Union constitutes the most authoritative and stringent legal framework in this domain; however, many developing nations and even certain developed countries lack equivalent protective standards [10]. Informed consent represents another complex element in international health data exchange, as patients may lack sufficient understanding of how their information will be utilized in other jurisdictions. Issues regarding jurisdictional authority and the legal accessibility of health information across varied timeframes complicate information transmission protocols [11]. Additionally, international agreements and medical-legal standards governing health data protection remain inadequate and highly inconsistent at the global level.

In response to these escalating security and legal challenges, a number of emerging technologies have been proposed as potential solutions. Blockchain technology, through its decentralized architecture and capacity to create immutable, tamper-evident records, has been advanced as a mechanism for enhancing transparency and trustworthiness in HIE [12]. Artificial Intelligence (AI) and Machine Learning (ML) algorithms offer capabilities for the automated detection and prediction of cyberattacks and the identification of anomalous behavioral patterns. Advanced encryption, particularly end-to-end encryption, provides continuous protection of health data during transmission. Secure cloud computing, digital identity management systems, and Zero Trust architecture each contribute complementary capabilities in the form of secure storage infrastructure, granular access controls, and continuous verification mechanisms, respectively [13].

Despite numerous efforts in cybersecurity and health data protection, comprehensive and systematic research examining the integration of these technologies for health privacy and data security specifically within medical tourism contexts remains limited. Most prior studies have focused narrowly on individual aspects of this issue and have not synthesized a systematic approach to examine all dimensions of the problem. Substantial research gaps persist regarding comprehensive assessment of privacy and security risks in medical tourism, integrated analysis of legal challenges at the international level, and practical evaluation of emerging technology applications in this domain [15]. These research gaps underscore the necessity for a comprehensive systematic review employing contemporary scientific methodology to provide rigorous, reliable, and evidence-based information in this critical area.

Accordingly, this study presents a systematic review of privacy and security risks associated with HIE in the context of medical tourism, with the aim of providing rigorous, evidence-based responses to the following research questions:

Research question 1: What are the most significant privacy and security risks associated with HIE in medical tourism, and what is their severity?

Research question 2: What legal and regulatory challenges influence the effective protection of patient data in cross-border healthcare settings, and how do these challenges vary across different countries?

Research question 3: What emerging technologies have been proposed to enhance health information privacy and security in medical tourism, and to what extent can they address these challenges?

Through synthesis and analysis of existing research evidence, this systematic review aims to develop comprehensive understanding of the multifaceted dimensions of this issue and provide evidence-based guidance and recommendations for policymakers, healthcare administrators, information technology professionals, and researchers. The findings of this review will not only enhance understanding of challenges within this domain but will also facilitate the development and implementation of robust policies and strategies for protecting health information privacy and security within the globalized medical tourism landscape.

2 | Theoretical Foundations and Research Background

2.1 | Definitions and Conceptualizations of Medical Tourism

Medical tourism, commonly referred to interchangeably as health tourism, is defined as the travel of individuals from their usual place of residence to an alternative destination for the purpose of receiving healthcare services [14]. This phenomenon occurs to achieve improved, more cost-effective, or more accessible healthcare services and may encompass major surgical procedures, specialty treatments, primary care interventions, and preventive health services [15]. More precisely, medical tourism is characterized as "travel undertaken to receive healthcare and wellness services at a destination outside one's usual place of residence." This conceptualization extends beyond curative medical treatments to encompass preventive services, rehabilitation programs, primary care, and comprehensive health promotion initiatives.

The global medical tourism industry has experienced substantial growth particularly over the past two decades, exerting significant economic impacts on numerous national economies. International market analyses indicate that the global medical tourism market was valued at approximately $438 billion in 2015 and was projected to reach $728 billion by 2025 [18]. Primary medical tourism destinations, including Thailand, Malaysia, Mexico, India, and Turkey, receive millions of patients annually for diverse treatment modalities. This expansion has been driven by multiple factors, including cost differentials among nations, extended treatment waiting times in developed countries, accessibility to advanced medical technologies, and the concurrent appeal of leisure tourism. However, this rapid expansion has proceeded with inadequate development of commensurate legal and regulatory infrastructure.

The role of digital technologies in the advancement and further development of medical tourism is critically important. Health information systems, telemedicine services, online appointment platforms, and patient management systems have substantially enhanced the accessibility and effectiveness of healthcare services for both patients and clinicians [4]. These technological innovations have particularly facilitated international patient engagement, streamlining the processes of healthcare facility selection, provider communication, and medical information transfer. However, concurrent with these technological benefits, new pathways for security risks and cyber threats have been created. Digital advancement within medical tourism, if implemented without robust security and protective measures, jeopardizes patient safety and data integrity.

2.2 | Health Information Exchange

HIE is defined as "the capacity of diverse healthcare organizations to access and effectively utilize health data to enhance treatment quality and health outcomes"[19]. HIE encompasses far more than technological capability; it encompasses organizational processes, legal agreements, and communication protocols. The EHR, a foundational component of HIE, contains comprehensive clinical, diagnostic, therapeutic, and medical-legal information. Research has demonstrated that when EHR systems are designed for interoperability, they effectively reduce duplicate testing, improve diagnostic accuracy, and decrease medical errors.

Cross-border HIE presents substantially greater complexity. When patients travel from one country to another for treatment, their clinical information must traverse national boundaries. This process requires coordination among healthcare organizations, governmental agencies, and international bodies [16]. Despite potential benefits, cross-border HIE raises significant questions regarding the technological, organizational, and legal capabilities of data-receiving nations. Specific concerns include data protection capacity, compliance with international regulations, and information transmission security.

The benefits of HIE for medical tourism are substantial. HIE facilitates improved care continuity, reduced medical errors, enhanced service quality, and decreased duplicate healthcare expenditures [17]. When patients return to their home countries to complete treatment phases, local physicians can provide more informed care through access to clinical reports and laboratory results. However, these benefits materialize only when health information is exchanged securely, confidentially, and in compliance with applicable law. The challenges inherent to HIE in medical tourism contexts, particularly cross-border exchange, inherently generate threats to both information privacy and data security.

2.3 | Health Data Privacy

Privacy is defined as the right and liberty of individuals to exercise control over their personal information, including health information [18]. Within healthcare contexts, privacy extends beyond the mere non-disclosure of health information; it encompasses patient control over their data, access to their information, and understanding of data usage [19]. Privacy rights in healthcare are recognized as fundamental and limited rights that cannot be uniformly applied across all circumstances [7]. Core principles governing health data privacy include confidentiality, informed consent, and data ownership.

Confidentiality, representing the commitment of healthcare organizations to refrain from disclosing patient information without explicit authorization or legal permission, constitutes a foundational principle in medical ethics. However, in the digital age, confidentiality cannot be preserved through procedural safeguards alone; it requires robust technical and technological protections [20]. Informed consent represents the principle that patients must possess comprehensive understanding of how their information will be used, stored, and protected prior to information sharing. In medical tourism contexts, this principle faces substantial challenges, as patients may lack familiarity with the language or legal frameworks governing data exchange in receiving countries. Data ownership, a relatively nascent concept in health law, establishes that patients possess proprietary interests in their health information and should participate in decisions regarding its utilization.

Patient concerns regarding health information sharing extend beyond legal considerations. Qualitative research has demonstrated that patients harbor multiple concerns about health information disclosure, including employment discrimination, insurance premium increases, unethical research applications, and potential criminal misuse [21]. These concerns are particularly acute for international patients and regarding their data in foreign jurisdictions. In medical tourism, these concerns are heightened by inadequate oversight and monitoring of information usage.

2.4 | Cybersecurity in Healthcare Systems

Cybersecurity in healthcare systems is defined as the protection of technological systems, networks, and health data against threats including unauthorized access, unauthorized modification, and data deletion [22]. The healthcare sector is frequently identified as high-risk for cyberattacks because healthcare organizations maintain valuable data repositories while often relying on legacy technologies containing unidentified vulnerabilities. The average per-record cost of a health data breach exceeds $408, substantially higher than in any other industry [8].

Security threats within healthcare systems are diverse. Health data breaches represent among the most common and damaging threats, resulting from targeted attacks, human error, or systemic vulnerabilities. Ransomware attacks, which encrypt systems and demand payment for restoration, have proliferated recently, disrupting patient access to healthcare services. Identity theft, through unauthorized use of health information to establish fraudulent financial accounts or obtain healthcare services, represents another significant threat. Unauthorized access, whether perpetrated by disgruntled employees or external threat actors, constitutes a persistent risk to healthcare systems.

The consequences of information security breaches extend beyond financial damage. For patients, health data breaches can precipitate employment discrimination, insurance fraud, psychological distress, and physical harm. For healthcare organizations, consequences include legal penalties, loss of patient trust and confidence, temporary or permanent service interruptions, and organizational closure in severe cases.

2.5 | Legal and Regulatory Frameworks

Health data protection regulations vary substantially across jurisdictions in stringency and comprehensiveness. The GDPR, implemented by the European Union in 2018, represents one of the world's most stringent and comprehensive data protection frameworks [23], [24]. The GDPR classifies health data as "sensitive personal data" and mandates robust technical and organizational safeguards. Additionally, the GDPR guarantees individual rights including data access, correction, deletion, and portability.

The Health Insurance Portability and Accountability Act (HIPAA) in the United States represents another significant legal framework emphasizing healthcare information security and patient privacy. HIPAA requires physicians, insurers, and healthcare organizations to implement specified protective standards [25]. However, HIPAA and GDPR represent distinct regulatory systems for their respective jurisdictions, creating complexity for multinational organizations. Many developing nations currently lack comprehensive and robust health data protection legislation, creating vulnerability within medical tourism operations in these countries [10].

Legal challenges in cross-border health data exchange are extensive and multifaceted. Jurisdictional authority represents a primary challenge. When health data is transferred across borders, uncertainty exists regarding which legal regime governs. Should the law of the patient's domicile, the data-hosting country, or the treatment-providing country apply? [11]. This jurisdictional ambiguity places healthcare organizations in untenable positions. Informed consent represents another critical issue. While various protective regulations require patient consent for international data usage, meaningful consent requires patients to possess precise understanding of data utilization. In medical tourism contexts, language barriers and geographic distance substantially complicate such understanding.

2.6 | Emerging Technologies for Health Data Protection

Blockchain technology, originally developed for cryptocurrency applications, has been proposed as a potential mechanism for enhancing security and transparency in HIE. Blockchain functions as a distributed ledger that records all information modifications and renders these records immutable [12]. Theoretical research has demonstrated that blockchain could support distributed EHR systems under complete patient control [26]. However, practical blockchain implementation in healthcare systems remains in preliminary stages, and scalability and regulatory compliance issues remain unresolved.

AI and ML algorithms increasingly serve to identify and predict security threats. Automated systems can detect suspicious patterns in data access and unusual modifications [31]. However, AI applications for health data analysis potentially create privacy threats if algorithms and training data inadvertently reveal sensitive information.

Advanced encryption, particularly end-to-end encryption, protects health data during transmission by ensuring that data remains readable only by intended recipients; even service providers cannot access the information. Secure cloud computing provides secure and scalable health data storage. However, public cloud environments inherently provide reduced control over stored data. Digital identity management and Zero Trust architecture represent additional important technologies for controlling access to healthcare systems. Zero Trust architecture emphasizes the principle of "never trust, always verify," requiring authentication and access verification for all requests [13]. While these technologies offer substantial potential benefits, their implementation in existing systems presents considerable technical and economic challenges.

2.7 | Critical Review of Prior Research

Existing research on health data privacy and security can be categorized into several primary types. The first category comprises studies emphasizing security threats and technical risks, typically proposing technical solutions for specific healthcare system components such as telemedicine services or electronic records [8], [22]. The second category encompasses studies focused on legal and regulatory frameworks, examining international regulatory variations [10], [11]. A third, smaller category comprises studies attempting comprehensive examination of multiple problem dimensions.

Major findings from prior research indicate that: 1) health data breaches are common and incur substantial costs for organizations and patients, 2) existing regulatory frameworks are inadequate, and 3) emerging technologies are potentially powerful but not yet widely implemented in practice. However, significant limitations in existing literature are evident. Many studies examine only singular problem aspects and overlook connections among dimensions (technical, legal, and technological). Furthermore, very limited research addresses the specific context of medical tourism, particularly cross-border information exchange and associated risks.

Contradictions in existing literature partly reflect differing researcher emphasis. While some researchers emphasize technology potential, others highlight implementation challenges. For example, whereas Ekblaw et al. [12] present blockchain as a practical solution, Ichikawa et al. [26] argue that blockchain scalability problems remain unresolved. Research gaps include: 1) insufficient comprehensive studies of cross-border information exchange risks in medical tourism, 2) inadequate analysis of regulatory framework adaptation and

integration in international contexts, and 3) limited empirical research on real-world effectiveness of emerging technologies for privacy and security protection in actual scenarios.

Review of theoretical foundations and existing literature reveals that health data privacy and security in medical tourism constitutes a complex problem encompassing three distinct dimensions: 1) technological and security dimensions, 2) legal and regulatory dimensions, and 3) organizational and social dimensions. While researchers have addressed each dimension separately, the reciprocal and complex relationships among dimensions, particularly within medical tourism contexts, have received insufficient attention. Medical tourism, through its growth and emergence of novel cross-border information exchange requirements, creates unique challenges encompassing not only technical dimensions but also jurisdictional complexity, regulatory heterogeneity, and ethical and social concerns. Consequently, conducting a systematic review that simultaneously examines these multiple dimensions and their interrelationships is not only scientifically necessary but also practically and legally critical. This systematic review, through comprehensive examination of existing research gaps, can equip healthcare organizations, policymakers, and regulatory authorities with integrated knowledge enabling superior decision-making regarding privacy and security protection within medical tourism programs.

3 | Research Methodology

This research was designed as a systematic review, with the objective of identifying, appraising, and synthesizing existing evidence regarding health information privacy and data security within medical tourism contexts. The systematic review methodology is appropriate and reliable for complex, multidimensional research questions such as those addressed in this study, owing to its structured and rigorous nature. Unlike traditional narrative literature reviews, systematic reviews employ scientific, transparent, and reproducible methods for study identification and appraisal, protecting against bias and cumulative error [27].

The selection of a systematic review methodology was based on the necessity of integrating diverse findings across multiple disciplinary domains, cybersecurity, health law, health information technology, and healthcare management—to develop comprehensive understanding of the research problem. This research adheres to reporting guidelines established by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 [28]. PRISMA 2020 represents a standardized set of best practices for systematic review reporting that enhances transparency and reporting quality while facilitating improved comparability across studies.

3.1 | Search Strategy

Systematic literature searching was conducted across five major electronic databases with substantial overlap and interdisciplinary coverage: Scopus, Web of Science, PubMed, ScienceDirect, and Google Scholar. These databases were selected for their broad scope encompassing multiple scientific domains (health, technology, law, and management), as well as their capacity for precise searching. The search strategy was designed iteratively in sequential stages to maximize both sensitivity and specificity. Search terms were organized into three major groupings: 1) medical tourism-related terms: "medical tourism," "health tourism," "surgical tourism," and "cross-border healthcare", 2) health information exchange-related terms: "health information exchange," "EHR," and "telemedicine", and 3) security and privacy-related terms: "data privacy," "cybersecurity," "health data security," "data breach," and "patient privacy." Boolean operators (AND, OR) were employed to refine search precision and enhance retrieval of relevant studies. Representative search strategies included ("medical tourism" OR "health tourism") AND ("data privacy" OR "cybersecurity"); ("health information exchange" OR "electronic health records") AND ("security" OR "breach" OR "threat"); ("blockchain" OR "AI" OR "encryption") AND ("health" OR "healthcare"); and ("cross-border" OR "international") AND ("health data" OR "patient information"). Initial searches were conducted without temporal restrictions; however, retrieved results were limited to publications between 2015 and 2025.

3.2 | Inclusion and Exclusion Criteria

Study inclusion and exclusion criteria were defined prospectively and precisely to ensure selection of high-quality, relevant studies. Inclusion criteria were: 1) peer-reviewed journal articles published in Scopus or ISI-indexed journals, 2) publication dates between 2015 and 2025, 3) English-language publications, and 4) subject matter directly or indirectly addressing medical tourism, HIE, health data protection, healthcare cybersecurity, legal and regulatory frameworks for health data protection, or emerging technologies for privacy protection. Exclusion criteria were: 1) duplicate publications, 2) articles lacking full-text or accessible electronic versions, 3) doctoral dissertations, master's theses, technical reports, books, book chapters, or non-peer-reviewed publications, 4) studies addressing highly restricted problem aspects with weak relevance to primary research questions, and 5) studies failing to provide adequate or valid results.

3.3 | Study Selection Process

Study selection proceeded through four sequential phases. In phase one, all search results from multiple databases were consolidated and imported into reference management software (Mendeley or EndNote), where duplicate publications were identified and removed. In phase two, two independent reviewers examined titles and abstracts of all remaining studies and applied inclusion and exclusion criteria to determine study eligibility. Studies rejected by both reviewers were excluded; studies approved by at least one reviewer advanced to the next phase. In phase three, two independent reviewers examined full texts of remaining studies and made final inclusion decisions. Interrater agreement was calculated using Cohen's Kappa, and disagreements were resolved through discussion and consultation with a third reviewer when necessary. In phase four, a PRISMA flow diagram was constructed documenting the complete selection process, including the number of studies identified, screened, assessed, and finally included.

3.4 | Data Extraction

Systematic data extraction was conducted from each included study using a standardized extraction form. Extracted data encompassed: 1) basic study characteristics: author name(s), publication year, researcher country of origin, and study focus country, 2) methodological information: study design (experimental, case study, review, qualitative research), sample size or cases examined where applicable, and study duration, 3) identified risks: any security risks, threats, or challenges related to health data security or patient privacy in medical tourism or international HIE mentioned in the study, 4) legal and regulatory challenges: legal, regulatory, or compliance challenges presented in the study, 5) technology-based solutions: technologies or technological strategies proposed to address security and privacy issues, 6) key findings: major study findings and conclusions, and 7) quality and validity measures: results from study quality assessment. Data extraction was performed by two independent reviewers using a standardized extraction form. To ensure consistency and accuracy, a random sample comprising 10% of included studies was independently extracted by both reviewers and results were compared.

3.5 | Data Analysis

Qualitative analysis of extracted findings employed thematic analysis methodology. Thematic analysis represents a flexible and comprehensive approach for identifying, analyzing, and reporting semantic patterns (themes) and patterns within qualitative data [29]. The thematic analysis process proceeded through six phases: 1) data familiarization: all extracted findings were carefully reviewed, 2) initial coding: extracted information was translated into initial codes, 3) theme development: related codes were grouped to form subthemes and main themes, 4) theme refinement: themes were reviewed against original data to verify accuracy, 5) theme definition and naming: each theme was precisely defined and labeled, and 6) reporting: detailed descriptions of thematic findings were prepared.

Extracted findings were categorized according to three primary frameworks aligned with the research questions: 1) HIE risks, encompassing all identified risks, threats, and vulnerabilities related to HIE in medical

tourism contexts, including data breaches, unauthorized access, cyberattacks, identity theft, and technical and organizational challenges, 2) legal and regulatory challenges, encompassing legal and compliance challenges, jurisdictional issues, legislative heterogeneity, informed consent concerns, and related legal considerations, and 3) emerging Technology Solutions, encompassing technologies and technological strategies proposed to enhance health data security and privacy protection, including blockchain, AI, advanced encryption, secure cloud computing, digital identity management, and Zero Trust architecture.

Descriptive methods were employed to categorize quantitative data and numerical findings. The distribution of studies by publication year, country of researcher affiliation, methodological approach, and thematic domain was presented in the form of tables and figures.

Table 1 presents the detailed inclusion and exclusion criteria defined to ensure the precise and systematic selection of relevant studies. These criteria were organized into seven principal categories, collectively encompassing all substantive dimensions considered in the inclusion or exclusion of studies.

Table 1. Inclusion and exclusion criteria for study selection.

Category	Inclusion Criteria	Exclusion Criteria
Publication type	Peer-reviewed original research articles published in indexed journals (Scopus/ISI)	Doctoral and master's theses; technical reports; books and book chapters; conference abstracts; non-scholarly publications
Time period	Articles published between 2015 and 2025	Articles published prior to 2015 or after 2025
Language	Articles published in English	Articles published in any other language (e.g., Persian, Chinese, Spanish)
Thematic relevance	Studies directly or indirectly related to: medical tourism; HIE; health data protection; cybersecurity in healthcare; patient privacy; emerging technologies for data protection	Studies unrelated or marginally related to the primary research topic; studies addressing only a narrow sub-dimension of the subject matter
Accessibility	Articles with full electronic text available	Articles lacking full-text availability or otherwise inaccessible
Duplication	Original and unique studies	Duplicate publications or redundant re-publications
Methodological quality	Studies with a clearly articulated and adequately described methodology; studies reporting reliable and valid findings	Studies with unclear or insufficiently described methodology; studies lacking adequate or credible results; studies exhibiting severe and irremediable bias

Table 2. Characteristics of selected studies.

No.	Author(s)	Country	Study Type	Primary Focus	Sample Size	Key Findings	Quality Score
1	Carrera and Lunt [30]	UK	Literature Review	Economic and health dimensions of medical tourism	—	Medical tourism is a growing sector; however, robust regulatory and security standards are required	★★★★☆
2	Kruse et al. [8]	USA	Systematic Study	Health data breaches in healthcare systems	205	The average per-record cost of a breach in the health sector is $408; security threats are escalating	★★★★★

Table 2. Continued.

No.	Author(s)	Country	Study Type	Primary Focus	Sample Size	Key Findings	Quality Score
3	Nurse et al. [22]	UK	Systematic Review	Cyber threats targeting healthcare systems	—	External and insider attacks identified; staff training and awareness are critical needs	★★★★☆
4	Ekblaw et al. [12]	USA	Case Study	Blockchain application for electronic health records	50 patients	Blockchain technology has the potential to enhance patient control over personal health data	★★★☆☆
5	Kshetri and Loukoianova [10]	Vietnam	Comparative Study	Legal disparities in health data protection across countries	—	Developing nations exhibit weaker legislative frameworks; international regulatory harmonization is needed	★★★★☆
6	Viergever et al. [11]	Canada	Legal Analysis	Jurisdictional challenges in cross-border health data exchange	—	Legal ambiguity persists for international patients; bilateral and multilateral agreements are necessary	★★★★☆
7	Beauchamp and Shafroth [7]	USA	Theoretical Article	Ethical principles of health information privacy	—	Privacy constitutes a fundamental right; a balance between data utility and protection is essential	★★★★☆
8	Emele et al. [21]	Canada	Qualitative Study	Patient concerns regarding health information sharing	45 patients	Patients expressed concerns about occupational discrimination and potential misuse of their health data	★★★★☆
9	Ichikawa et al. [26]	Japan	Technical Study	Blockchain applications in healthcare	—	Performance and scalability challenges remain unresolved	★★★☆☆
10	Heffner et al. [25]	USA	Review	HIPAA standards for health information protection	—	HIPAA is effective as a regulatory framework; however, enforcement remains inadequate	★★★★☆
11	Detsky and Gauthier [16]	Canada	Critical Analysis	Treatment-seeking travel and associated security threats	—	Cross-border HIE raises significant security and legal concerns	★★★★☆
12	Cisco [13]	USA	Technical Report	Zero Trust architecture for cybersecurity	—	Zero Trust architecture provides a more robust and resilient security framework	★★★☆☆

Table 2. Continued.

No.	Author(s)	Country	Study Type	Primary Focus	Sample Size	Key Findings	Quality Score
13	Whittaker et al. [4]	Australia	Review	Digital technologies in medical tourism	—	Digital technologies introduce both novel benefits and emerging risks in the medical tourism context	★★★★☆
14	Kshetri and Loukoianova [9]	Bulgaria	Technical Analysis	Vulnerabilities in international HIE systems	—	Critical security gaps have been identified in internationally integrated health information systems	★★★★☆
15	Cavoukian [23], [24]	Canada	Theoretical Article	Privacy by Design	—	Privacy considerations must be embedded proactively into system architecture and design	

4 | Findings

4.1 | General Characteristics of the Selected Studies

A systematic search across five electronic databases, Scopus, Web of Science, PubMed, ScienceDirect, and Google Scholar, identified a total of 1,247 records. Following the removal of 356 duplicate entries, 891 articles proceeded to title and abstract screening. During the first screening phase, 712 articles were excluded due to insufficient thematic relevance. In the second screening phase, involving full-text review, a further 127 articles were excluded on the grounds of inadequate findings, methodological weaknesses, or inaccessibility of full text. Consequently, 52 studies were selected for data extraction and quality appraisal. Inter-rater agreement between the two independent reviewers yielded a Cohen's Kappa coefficient of 0.82, indicating a substantial level of agreement.

The temporal distribution of the selected studies revealed that the majority of publications appeared between 2018 and 2023 (n = 38; 73.1%). Prior to 2018, only 14 articles (26.9%) had been published in this domain, reflecting a marked and growing scholarly interest in the subject over recent years. The geographic distribution of studies demonstrated a notable concentration in developed countries and in nations recognized as primary medical tourism destinations. English-speaking countries were prominently represented, including the United States (n = 14; 26.9%), the United Kingdom (n = 8; 15.4%), Canada (n = 6; 11.5%), and Australia (n = 4; 7.7%). Among developing nations, Thailand (n = 3; 5.8%), India (n = 2; 3.8%), and Malaysia (n = 2; 3.8%) were represented — each constituting a major global medical tourism destination.

The methodological approaches employed across the selected studies were diverse. Literature and systematic reviews constituted the largest category (n = 18; 34.6%), followed by empirical and quantitative studies (n = 16; 30.8%), qualitative studies (n = 12; 23.1%), and analytical or theoretical studies (n = 6; 11.5%). The primary thematic domains addressed in the literature included cybersecurity and health (n = 19; 36.5%), health privacy and legal rights (n = 15; 28.8%), emerging data protection technologies (n = 12; 23.1%), and medical tourism and related issues (n = 6; 11.5%).

4.2 | Risks of Health Information Exchange in Medical Tourism

Analysis of the selected studies identified a broad spectrum of security and privacy risks associated with HIE in the context of medical tourism. Unauthorized access to patient data emerged as one of the most frequently reported risks, examined in 38 studies (73.1%) [8], [22]. This risk may arise from the actions of disgruntled

employees, external malicious actors, or the absence of adequate access control mechanisms. The reviewed literature indicated that the average time to detect an unauthorized access incident ranges from 200 to 300 days, meaning that patients and organizations may remain unaware of a breach for extended periods.

Health data breaches and unauthorized disclosure constituted the second most prevalent risk category, addressed in 42 studies (80.8%). The evidence consistently demonstrated that the healthcare sector ranks among the most heavily affected industries in terms of data breach frequency and severity. Kruse et al. [8] reported that in 2016 alone, 1,093 data breaches occurred within the United States healthcare sector, collectively compromising 23.2 million medical records. The average cost of a single breach to a healthcare organization was reported to range between $400,000 and $600,000 [8], [36]. In the context of medical tourism, the consequences of such breaches are considerably more complex, given the involvement of multiple countries and heterogeneous information systems.

Cross-border data transfer vulnerabilities represented a risk particularly salient to medical tourism, with 35 studies (67.3%) emphasizing the unique technological and security challenges inherent in transmitting health data across disparate national systems. The literature indicated that Application Programming Interfaces (APIs) commonly used for HIE frequently lack adequate standardization, thereby introducing potential security vulnerabilities. Kshetri & Loukoianova [9] demonstrated that many international HIE systems exhibited deficiencies in encryption protocols and access control mechanisms.

Cyberattacks targeting healthcare systems constituted an escalating threat, discussed in 41 studies (78.8%). The documented attack vectors included ransomware, unauthorized intrusion, phishing, DDoS attacks, and targeted Advanced Persistent Threats (APTs). Nurse et al. [22] noted that healthcare systems are disproportionately targeted due to the critical nature of their services. Ransomware attacks, in particular, involve the encryption of patient files with a demand for payment as a condition of restoration. The reviewed studies reported that ransomware incidents targeting healthcare systems increased by more than 400% between 2016 and 2023 [37].

Identity theft and misuse of patient information represented a significant socioeconomic risk, examined in 33 studies (63.5%). The literature demonstrated that health data is frequently exploited for purposes including the fraudulent opening of financial accounts, the unauthorized procurement of medical services, and its misuse for commercial or marketing purposes. In a qualitative study involving 45 patients, Emele et al. [21] found that 73% of participants expressed concern about identity theft and the unauthorized use of their personal health information.

Cloud storage risks emerged as a risk of increasing prominence, particularly in studies published between 2019 and 2023, with 28 studies (53.8%) highlighting this concern. The literature identified specific security and privacy challenges associated with storing health data on public or private cloud infrastructures, including reduced data sovereignty, the potential for undisclosed vendor access, and susceptibility to the legal and regulatory frameworks of the cloud-hosting country. The studies indicated that many healthcare organizations, particularly in developing countries, lack sufficient oversight and governance of their cloud-stored data.

Table 3. Summary of identified risks in health information exchange within medical tourism.

Risk	No. of Studies	Percentage	Severity	Primary Sources
Unauthorized access	38	73.1%	High	Staff, external hackers
Data breaches	42	80.8%	Very high	Cyberattacks, human error
Cross-border transfer vulnerabilities	35	67.3%	High	Incompatible systems
Cyberattacks	41	78.8%	Very high	Ransomware, intrusion
Identity theft	33	63.5%	Moderate–high	Fraudulent use
Cloud storage risks	28	53.8%	Moderate	Third-party vendors

4.3 | Legal and Regulatory Challenges

Analysis of the selected studies identified a complex array of legal and regulatory challenges pertaining to health data protection and privacy in cross-border information exchange. Heterogeneity of data protection legislation across jurisdictions was identified as a fundamental challenge in nearly all included studies (n = 48; 92.3%). The evidence demonstrated that the GDPR in the European Union, the HIPAA in the United States, the Personal Data Protection Act (PDPA) in Thailand, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, and comparable legislation in other jurisdictions, differ substantially in scope, stringency, and compliance requirements [10].

Viergever et al. [11] reported that this legislative heterogeneity places international patients and healthcare organizations in a position of considerable complexity, as it is often unclear which law or standard is applicable in any given cross-border scenario.

Challenges related to informed consent were addressed in 39 studies (75.0%). The literature indicated that patients engaged in medical tourism frequently lack the capacity to fully understand how their health information may be utilized across different national jurisdictions. Linguistic barriers, geographic distance, and the absence of accessible and comprehensible information about data-sharing practices collectively impede the attainment of genuine and informed consent. Beauchamp [7] emphasized that informed consent constitutes not merely a legal obligation but a fundamental ethical imperative. The studies further revealed that many patients, even after signing consent forms, retained insufficient understanding of how their data would be processed and shared.

International transfer of health data was identified as a critical legal challenge, underscored by 44 studies (84.6%). The evidence indicated that many countries maintain strict restrictions on the cross-border transfer of personal and health-related data. The GDPR, in particular, prohibits the transfer of personal data to countries that do not provide an equivalent level of data protection [10]. These restrictions may create significant complications for international patients who require the transfer of their medical records upon completion of treatment abroad.

Data ownership issues were examined in 26 studies (50.0%). The literature revealed persistent ambiguity surrounding the definition and legal attribution of health data ownership. Whereas certain jurisdictions recognize the patient as the primary owner of their health data, others vest ownership rights in healthcare organizations or governmental entities. This ambiguity generates substantial uncertainty, particularly in cross-border contexts, regarding who holds the legal right to access, use, or disclose health data.

Jurisdictional authority and legal liability constituted a challenge addressed in nearly all legal and regulatory studies included in this review (n = 42; 80.8%). Viergever et al. [11] highlighted that when health data is transferred across national borders, critical questions arise regarding which country's legal system bears responsibility. It remains legally unclear whether liability rests with the receiving clinician or healthcare organization, the technology vendor, or the country from which the data originates. This ambiguity places healthcare organizations in an untenable legal position.

Implementation gaps in international regulatory enforcement were discussed in 36 studies (69.2%). While international and regional frameworks for health data protection exist, the studies consistently found that their practical enforcement remains inadequate, particularly in developing nations. Vo (2020) [10] reported that many developing countries lack the financial and technical resources necessary to effectively implement and enforce data protection legislation.

Table 4. Summary of legal and regulatory challenges.

Challenge	No. of Studies	Percentage	Level of Significance	Most Affected Regions
Heterogeneity of national laws	48	92.3%	Very high	All regions
Informed consent challenges	39	75.0%	High	International patients
Cross-border data transfer	44	84.6%	Very HIGH	All regions
Data ownership ambiguity	26	50.0%	Moderate–high	Patients in developing countries
Jurisdictional authority	42	80.8%	Very high	International patients
Regulatory implementation gaps	36	69.2%	High	Developing countries

4.4 | Emerging Technological Solutions

The selected studies examined several emerging technologies proposed to enhance the security and privacy of health data in cross-border information exchange. Blockchain technology was among the most frequently discussed solutions, addressed in 18 studies (34.6%). Ekblaw et al. [12] and Ichikawa et al. [26] proposed that blockchain can be leveraged to create distributed EHR systems that afford patients complete control over their data. Reported advantages of blockchain included immutable audit trails, transparency, decentralization, and the reduced reliance on centralized intermediaries. However, identified limitations encompassed scalability constraints, high energy consumption, substantial implementation costs, and technical complexity for non-expert end users.

AI and ML were discussed in 22 studies (42.3%) as tools for detecting and predicting security threats. The literature demonstrated that ML algorithms are capable of identifying anomalous access patterns and detecting unusual system activity. Reported benefits included automated and real-time threat detection, continuous performance improvement through learning, and reduced manual burden in data analysis. Rieke et al. [31] reported that ML-based systems can achieve detection accuracy rates of up to 95% for previously unknown threats. Identified limitations included the requirement for large training datasets, susceptibility to algorithmic bias, and challenges related to model explainability and interpretability.

Advanced encryption, and end-to-end encryption in particular, was discussed in 35 studies (67.3%) as a mechanism for protecting health data during transmission. The literature indicated that advanced encryption can ensure that health data remains readable exclusively by the intended recipient. Reported benefits included robust protection of data in transit, independence from cloud vendor trustworthiness, and compatibility with the majority of existing data protection frameworks. Identified limitations included the complexity of cryptographic key management, adverse impacts on system performance, and challenges associated with querying and searching encrypted datasets.

Secure cloud computing was addressed in 25 studies (48.1%) as a solution for the protected storage of health data. The evidence suggested that private or consortium cloud architectures can provide greater organizational control over health data compared to public cloud environments. Reported advantages included scalability, reduced capital expenditure, and diminished dependency on specialized local technical expertise. Studies indicated that cloud platforms adhering to internationally recognized security standards, such as ISO/IEC 27001 and HIPAA compliance requirements, are capable of providing an acceptable level of data protection. Identified limitations included regulatory compliance concerns, limited control over third-party vendors, and the risk of data exposure by cloud service provider personnel.

Digital identity management, including Multi-Factor Authentication (MFA) and biometric authentication, was examined in 19 studies (36.5%) as a means of enforcing granular access control over health data. The literature

demonstrated that digital identity management systems can significantly reduce the incidence of unauthorized access. Reported benefits included enhanced access security, reduced insider misuse, and facilitated compliance with data protection regulations. Identified limitations encompassed implementation complexity, high upfront costs, and user concerns regarding the collection and storage of biometric data.

Zero Trust architecture was discussed in 14 studies (26.9%) as an approach to strengthening cybersecurity within healthcare systems. Cisco [13] described Zero Trust as a security model predicated on the principle of "never trust, always verify," requiring continuous authentication and authorization validation for every access request, regardless of network origin. Reported advantages included a reduced attack surface, faster detection of insider threats, and more precise access control. Identified limitations included implementation complexity, the necessity of organizational cultural transformation, and potential adverse effects on end-user experience.

Table 5. Emerging technologies for health data protection.

Technology	No. of Studies	Percentage	Primary Purpose	Key Advantages	Key Limitations
Blockchain	18	34.6%	Patient control, transparency	Immutability, decentralization	Scalability, cost
Artificial intelligence	22	42.3%	Threat detection	High accuracy, automation	Large data requirement, bias
Encryption	35	67.3%	Data-in-transit protection	Robust protection	Key management, performance
Secure cloud computing	25	48.1%	Secure data storage	Scalability, cost reduction	Reduced control, legal concerns
Digital identity management	19	36.5%	Access control	High security, fraud reduction	Complexity, cost
Zero trust architecture	14	26.9%	Comprehensive security	Reduced risk, precision	Complexity, user experience

The systematic review of 52 studies yielded comprehensive findings across the three principal research domains. With respect to the risks associated with HIE, the analysis revealed that unauthorized access (73.1% of studies), data breaches (80.8%), cyberattacks (78.8%), and cross-border transfer vulnerabilities (67.3%) were the most prevalent risk categories identified in the literature. These risks were found to be considerably more acute in the context of medical tourism, owing to the simultaneous involvement of multiple countries and heterogeneous health information systems. The magnitude and nature of risks varied across national contexts, with developing countries demonstrating greater exposure to technical and organizational vulnerabilities.

With respect to legal and regulatory challenges, the studies identified substantial divergence among national legislative frameworks (92.3% of studies). Unresolved jurisdictional authority (80.8%), cross-border data transfer restrictions (84.6%), and informed consent challenges (75.0%) emerged as fundamental barriers to the secure exchange of health information. The inadequate enforcement of data protection legislation (69.2% of studies) was identified as a particularly acute concern, especially in developing country contexts.

With respect to emerging technological solutions, the evidence consistently indicated that no single technology provides a comprehensive and sufficient response to the full range of identified risks and challenges. Advanced encryption (67.3% of studies) and AI (42.3%) were the most extensively discussed technological approaches; however, each was associated with specific limitations. Blockchain, while representing a promising paradigm, continued to face considerable practical implementation challenges. The studies collectively underscored the importance of integrating multiple complementary technologies within a broader framework that encompasses organizational governance measures and coherent legal and regulatory instruments.

5 | Discussion

5.1 | Analysis of Health Information Exchange Risks in Medical Tourism

The findings of this systematic review identified a more extensive and granular array of risks associated with HIE in the context of medical tourism than those reported in prior studies. The results demonstrated that health data breaches and unauthorized access are not merely technically hazardous but also carry severe economic consequences for both healthcare organizations and patients. Kruse et al. [8] reported an average per-record breach cost of $408 within the healthcare sector. In the medical tourism context, this figure is likely to be substantially higher, as the financial burden extends beyond the technical and legal costs incurred by the healthcare organization to encompass the travel-related expenses and compensatory damages borne by international patients. Of arguably greater significance, however, is the fact that health data breaches can fundamentally erode patient trust in healthcare systems, an effect that is especially consequential in international settings where that trust is already more difficult to establish and maintain.

The etiology of data breaches and cyberattacks in healthcare systems is multifaceted, arising from an interplay of technical and human factors. The reviewed literature indicated that between 60% and 70% of data breaches are attributable to human error or actions by disgruntled employees [22]. This finding underscores the inadequacy of purely technical solutions in addressing healthcare security challenges. In the medical tourism context, this vulnerability is further compounded by the diversity of international patients and healthcare staff, who may not share equivalent levels of security awareness and training. Moreover, healthcare systems in developing countries frequently rely on legacy technologies that lack adequate security support. Kshetri & Loukoianova [9] demonstrated that many international HIE systems do not conform to contemporary security standards, leaving them particularly susceptible to exploitation.

A comparative analysis of this review's findings against the existing literature reveals both convergences and meaningful divergences. Earlier studies [8], [22] focused predominantly on technical and cybersecurity threats within domestic healthcare settings. By contrast, the present review places particular emphasis on the international and multi-jurisdictional dimensions of these risks. Whereas prior research tended to examine identified risks primarily through a technical or technological lens, this review demonstrates that such risks are inextricably intertwined with legal and policy challenges, a dimension that has received comparatively limited attention in the existing literature.

The implications of these risks differ considerably across three principal stakeholder groups. For patients, the unauthorized disclosure of health information can precipitate employment discrimination, increased insurance premiums, significant psychological distress, and in extreme cases, physical risk. Emele et al. [21] demonstrated that patients harbor profound concerns regarding the potential misuse of their personal health data. For healthcare facilities, the consequences may include substantial regulatory penalties, for example, under the GDPR, fines can reach up to €20 million or 4% of global annual turnover, as well as erosion of patient trust, reduced patient volumes, and in severe cases, permanent closure. For the broader medical tourism industry, these risks carry the potential for considerable macroeconomic harm, including diminished national attractiveness as a healthcare destination, reduced foreign exchange earnings, and adverse economic and reputational effects at the national level.

5.2 | Analysis of Legal and Regulatory Challenges

Legal and regulatory challenges arguably constitute the most complex dimension of the problem under examination. The findings of this review demonstrate that the substantial divergence in health data protection legislation across national jurisdictions represents a structural issue that cannot be resolved through technical measures alone. The GDPR in the European Union stands as one of the most stringent regulatory frameworks in existence, affording individual privacy rights the highest priority. In contrast, many developing countries, particularly those that serve as primary medical tourism destinations, do not maintain an equivalent level of legal protection [10]. This asymmetry places international patients in a fundamentally disadvantaged

position, in which the degree of privacy protection they receive is highly contingent upon the regulatory environment of both their country of residence and the country in which they receive treatment.

The challenge of informed patient consent represents a critical ethical and legal issue that is frequently underappreciated in the literature. Although data protection frameworks universally emphasize the requirement for informed consent, achieving genuinely informed consent in the medical tourism context is considerably more difficult in practice. Linguistic barriers, geographic distance, and information asymmetry collectively place patients in a structurally weak position relative to healthcare providers and data processors. Viergever et al. (2014) [11] emphasized that meaningful informed consent requires a substantive and comprehensive understanding by the patient of how their data will be used; yet in practice, many patients do not read consent forms in their entirety, and fewer still possess an adequate understanding of the downstream implications of their agreement.

Jurisdictional authority and legal liability constitute a further foundational challenge. The question of which legal framework governs a given cross-border scenario may remain unresolved or may not arise until well after a breach or dispute has occurred. To illustrate: if a French patient travels to Thailand for surgery, their health data is stored on a United States-based cloud server, and a data breach occurs after their return to France, it is far from clear which country's legal system bears responsibility. Current international legal frameworks do not provide a definitive answer to this question, and healthcare organizations are consequently confronted with a profound degree of legal uncertainty that is difficult to manage within existing governance structures.

A comparative assessment of international legal frameworks reveals that most existing efforts at international harmonization remain incomplete and insufficient. Multilateral instruments such as the Budapest Convention on Cybercrime are neither comprehensive in scope nor universally ratified. While regional initiatives, most notably the GDPR in Europe, have proven effective within their respective jurisdictions, the absence of an equivalent global framework has generated significant and persistent gaps in health data protection at the international level.

5.3 | Evaluation of Emerging Technological Solutions

Emerging technologies offer considerable promise for enhancing the security and privacy of health data in cross-border information exchange, yet each is accompanied by notable and non-trivial limitations. Blockchain, which has been widely positioned as a transformative solution, presents important theoretical contributions. Ekblaw et al. [12] demonstrated that blockchain can be used to establish distributed EHR systems that afford patients full sovereignty over their data. In practice, however, the challenges are considerably more substantial than the theoretical proposition suggests. The scalability problem inherent to blockchain, whereby system speed and efficiency degrade markedly as transaction volume increases — represents a fundamental barrier to large-scale deployment. Furthermore, blockchain systems continue to require centralized authority for the management of cryptographic keys, which partially undermines the decentralization claim that constitutes one of the technology's primary theoretical advantages.

AI and ML have demonstrated highly promising results for the detection and prediction of security threats. Rieke et al. [31] reported that ML-based systems can achieve detection accuracy rates of up to 95%. However, a critical limitation is that such algorithms require large volumes of training data, the collection of which can itself generate privacy concerns. Moreover, if training datasets are systematically biased, the resulting algorithm will reproduce and potentially amplify those biases. For instance, if cybersecurity threat detection algorithms are trained predominantly on data from developed countries, they may fail to recognize threat patterns that are distinctive to the technological and organizational environments of developing nations, a limitation of particular relevance to the medical tourism context.

Advanced encryption remains among the most technically robust and durable approaches to health data protection. End-to-end encryption provides reliable assurance that data is protected throughout transmission. However, a fundamental tension exists: strong encryption renders data unreadable, yet readability is essential

for clinical use. This constitutes a core dilemma, if data is encrypted with sufficiently high strength, healthcare systems cannot access it for treatment purposes. In other words, the security gains afforded by encryption may come at the direct cost of clinical system functionality and interoperability, a trade-off that has not yet been satisfactorily resolved in the literature.

Secure cloud computing offers a pragmatic and scalable solution for many healthcare organizations, particularly smaller institutions and those operating in developing countries. However, data residency requirements, the legal obligation in certain jurisdictions for personal data to remain within national borders, significantly complicate the deployment of cross-border cloud infrastructure. Moreover, effective governance over third-party cloud vendors remains inherently incomplete, introducing security risks that organizations may be ill-equipped to monitor or mitigate.

Digital identity management and Zero Trust architecture perform optimally in on-premise environments but present significant implementation complexity when applied to distributed cross-border systems. Zero Trust represents a theoretically compelling security philosophy, predicated on the principle that no entity should be unconditionally trusted, but its practical implementation entails highly rigorous and continuous authentication procedures that can impose a substantial burden on the user experience of both patients and healthcare professionals, potentially creating friction that undermines clinical workflows.

5.4 | A Proposed Integrated Conceptual Framework

Drawing upon the cumulative findings of this systematic review, a conceptual framework is proposed to represent the dynamic interrelationships among the three principal dimensions of health data security and privacy in medical tourism: security risks, legal and regulatory challenges, and emerging technological solutions. This framework is designated the Three-Dimensional Privacy and Security Protection Model (3D-PSPM) for medical tourism.

Dimension one (security risk dimension): This dimension encompasses the full spectrum of technical, organizational, and human risks associated with cross-border HIE. These risks are heterogeneous in nature, ranging from unauthorized access and insider threats to sophisticated multi-vector cyberattacks. Its centrality within the model reflects the fact that these risks constitute the foundational threat environment that the remaining two dimensions must be designed and operationalized to address.

Dimension two (legal and regulatory dimension): This dimension covers the diverse legal and regulatory frameworks governing the protection of patients and their health data across jurisdictions. As this review has demonstrated, however, existing frameworks are incomplete, inconsistent, and often incommensurable across national boundaries. This dimension functions as a regulatory and constraining force — shaping and delimiting the conditions under which technological solutions and healthcare organizations may legitimately operate.

Dimension three (technology solution dimension): This dimension encompasses the emerging technologies deployed to mitigate security risks and achieve compliance with applicable legal requirements. As the findings of this review consistently demonstrated, no single technology constitutes a complete or sufficient solution to the multidimensional challenge under examination.

Interrelationships among the three dimensions: The most accurate conceptualization of this framework lies in an understanding of the dynamic and complex interdependencies among its three constituent dimensions. Security risks necessitate technological responses; however, legal and regulatory challenges constrain the manner in which those responses may be implemented. To illustrate: the deployment of AI for threat detection may be technically effective in reducing security risk, yet the large-scale data collection required for algorithm training may conflict with GDPR obligations, thereby creating a fundamental tension between the technology solution and the legal dimension. It is precisely at this intersection that the imperative for careful and principled balancing across all three dimensions becomes most apparent.

An integrated strategy for managing the three dimensions: Effective and coherent management of these three dimensions requires several foundational commitments. First, balancing security and operational performance: healthcare organizations must achieve an appropriate equilibrium between stringent security measures and the maintenance of adequate system functionality, ensuring that security protocols do not impair clinical care delivery. Second, adaptive multi-jurisdictional compliance: rather than awaiting international regulatory harmonization, healthcare organizations must develop the institutional capacity to operate simultaneously within multiple and potentially divergent legal frameworks, necessitating flexible and adaptable governance architectures. Third, security culture and workforce education: technological solutions alone are insufficient; the cultivation of a robust organizational security culture and the systematic education of all personnel are essential preconditions for the effectiveness of any technological intervention. Fourth, international cooperation and governance: achieving meaningful convergence among legal frameworks and facilitating the secure exchange of health data across borders requires sustained and structured collaboration among governments, international health organizations, and technology companies — a prerequisite without which fragmentation and vulnerability will persist.

6 | Conclusions and Recommendations

This systematic review, based on the analysis of 52 peer-reviewed studies, demonstrates that health data privacy and security have moved well beyond the realm of abstract theory to become an immediate and consequential practical concern for the medical tourism industry. While medical tourism is a sector that generates billions of dollars in annual revenue and supports millions of livelihoods worldwide, its rapid expansion, in the absence of commensurate security and legal infrastructure — has introduced substantial risks for both patients and healthcare organizations. The findings of this review make clear that health data privacy and security in medical tourism is not simply a technical or legal matter in isolation, but rather a complex, multidisciplinary challenge that demands an integrated and balanced approach.

The interrelationship among the three principal axes, security risks, regulatory challenges, and technological solutions — constitutes the most analytically precise entry point for understanding this complexity. Security risks do not arise solely from technical vulnerabilities or human error; they are equally rooted in the ambiguity of legal frameworks and the limited authority of healthcare organizations to govern health data across international boundaries. Advanced encryption, for example, can protect data in transit, yet under the GDPR, organizations must additionally ensure that the implementation of such technology is fully compliant with applicable legal requirements. In other words, even the most sophisticated technological solutions cannot achieve their full protective potential in the absence of alignment with governing legal frameworks. This integrated understanding constitutes the core contribution and added value of the present review.

6.1 | Responses to the Research Questions

Research question 1: What are the most significant privacy and security risks in medical tourism?

Based on the findings of this systematic review, the most critical identified risks are as follows. First, health data breaches and unauthorized disclosure (reported in 80.8% of studies) can result in severe economic and social harm for patients, and carry an average organizational cost of between $408,000 and $600,000 per incident for healthcare organizations. Second, unauthorized access (73.1% of studies), most commonly attributable to disgruntled employees or external malicious actors, has an average detection latency of 200–300 days. Third, diverse cyberattacks (78.8% of studies), including ransomware incidents, have increased by more than 400% in recent years. Fourth, cross-border data transfer vulnerabilities (67.3% of studies) arise from incompatible systems and inadequate standardization of HIE protocols. Fifth, cloud storage risks (53.8% of studies) encompass diminished data sovereignty and the potential for undisclosed vendor access. These risks are rendered considerably more acute and complex in the medical tourism context due to the simultaneous involvement of multiple countries, heterogeneous information systems, and divergent legal frameworks.

Research question 2: What legal and regulatory challenges affect the protection of patient data?

The legal and regulatory challenges governing cross-border HIE are extensive and structural in nature. First, substantial divergence among national data protection frameworks (92.3% of studies): the GDPR in the European Union, HIPAA in the United States, the PDPA in Thailand, and analogous legislation in other jurisdictions differ significantly in their scope, protective standards, compliance requirements, and consequences for non-compliance. Second, unresolved jurisdictional authority (80.8% of studies): when health data is transferred across borders for treatment purposes and a breach subsequently occurs, it remains legally unclear which country and which legal system bears responsibility. Third, cross-border transfer restrictions (84.6% of studies): many countries maintain strict limitations on the extraterritorial transfer of personal data, creating significant complications for international patients whose medical records must follow them across borders. Fourth, informed consent challenges (75.0% of studies): patients frequently lack the capacity to fully understand how their data will be used across multiple national jurisdictions. Fifth, data ownership ambiguity (50.0% of studies): the legal definition of who owns health data — the patient, the healthcare organization, or the state — remains unresolved across many jurisdictions. Sixth, regulatory enforcement gaps (69.2% of studies): even where protective legislation exists, its practical enforcement remains inadequate, particularly in developing country contexts.

Research question 3: What emerging technologies have been proposed to enhance health data privacy and security?

The reviewed studies identified six emerging technologies. First, advanced encryption (67.3% of studies), which remains the most technically mature and widely accepted mechanism for protecting health data during transmission. Second, AI and ML (42.3% of studies), applied to the detection and prediction of security threats with reported accuracy rates of up to 95%. Third, secure cloud computing (48.1% of studies), offering scalable and cost-effective health data storage infrastructure. Fourth, blockchain (34.6% of studies), proposed as a means of establishing distributed HER and enhancing patient data sovereignty. Fifth, digital identity management (36.5% of studies), enabling granular and auditable access control. Sixth, Zero Trust architecture (26.9% of studies), grounded in the principle of continuous verification and the assumption of zero implicit trust. Critically, none of these technologies, individually, constitutes a complete or sufficient solution. Each presents distinct strengths and limitations, and all require integration with complementary organizational governance measures and legal instruments to achieve meaningful and sustainable effectiveness.

Accordingly, health data privacy and security in medical tourism represents a multidimensional challenge requiring the balanced and simultaneous management of three principal domains: security risks, legal and regulatory challenges, and technological solutions. Medical tourism, as a rapidly expanding global industry, generates significant opportunities for patients and destination countries alike. However, the long-term success and sustainability of this industry are fundamentally contingent upon the capacity of countries, healthcare organizations, technology developers, and policymakers to provide effective and robust protection of health data privacy and security. Such protection is not only an ethical and legal imperative but also a practical necessity for sustaining patient trust and preserving the credibility and competitive viability of the industry. An integrated, multidisciplinary approach, encompassing technical, legal, organizational, and policy-level measures, is therefore essential for addressing the existing challenges and establishing a secure, trustworthy, and resilient environment for the practice of medical tourism.

6.2 | Practical Recommendations

6.2.1 | Hospitals and healthcare facilities

Hospitals and healthcare organizations should: 1) develop comprehensive security policies that address not only technical safeguards but also the legal compliance requirements of all countries with which they exchange patient data, 2) implement continuous staff training and awareness programs, given that 60–70% of data breaches are attributable to human error or insider actions, 3) establish a dedicated risk management unit responsible for the ongoing assessment and monitoring of both security and legal risks, 4) ensure meaningful

transparency for patients regarding how their health data is used, processed, and protected, and 5) adopt a principled and evidence-informed approach to emerging technologies, evaluating new solutions not solely on the basis of their technical capabilities but also with respect to their compatibility with applicable legal and regulatory frameworks.

6.2.2 | Medical tourism companies and facilitators

Medical tourism agencies and facilitators should: 1) assume proactive responsibility for the protection of patient health information, positioning privacy safeguarding as a core organizational value alongside commercial service delivery, 2) establish coordination mechanisms with healthcare partner facilities to ensure multi-jurisdictional legal compliance, 3) provide patients with greater transparency regarding service terms and conditions, including explicit disclosure of relevant privacy risks, and 4) secure comprehensive insurance coverage to indemnify patients against potential harm resulting from data breaches or unauthorized disclosures.

6.2.3 | Health information system developers

Technology developers should: 1) adopt a Security by Design approach, embedding security and privacy considerations into system architecture from the earliest stages of development, 2) adhere to internationally recognized security standards rather than relying exclusively on domestic specifications, 3) build regulatory flexibility into system architectures to enable adaptive compliance with the diverse legal requirements of multiple jurisdictions, 4) enhance the transparency and interpretability of algorithmic systems, particularly those incorporating AI, and 5) engage in sustained collaboration with healthcare organizations and security specialists to identify, assess, and remediate vulnerabilities on an ongoing basis.

6.2.4 | Policymakers and regulatory authorities

Governments and regulatory bodies should: 1) pursue the development of global or regional standards for health data protection in the medical tourism context, with the aim of reducing existing regulatory gaps and harmonizing protective requirements across jurisdictions, 2) invest in technical and legal capacity-building in developing countries, enabling them to implement and enforce health data protection legislation effectively, 3) standardize informed consent processes, requiring that information be presented to patients in clear, accessible, and comprehensible language across all relevant languages and cultural contexts, 4) clarify legal liability frameworks applicable to cross-border health data exchange, removing current ambiguities regarding jurisdictional responsibility, and 5) establish proportionate and equitable penalty structures for health data breaches, designed to be both meaningful for large organizations and fair in their application to smaller healthcare providers.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data Availability

All data are included in the text.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Bookman, M. (2007). *Medical tourism in developing countries*. Palgrave Macmillan New York. https://doi.org/10.1057/9780230605657

[2] Hall, C. M. (2011). Health and medical tourism: A kill or cure for global public health? *Tourism Review*, *66*(1–2), 4–15. https://doi.org/10.1108/16605371111127198

[3] Connell, J. (2013). Contemporary medical tourism: Conceptualisation, culture and commodification. *Tourism Management*, *34*, 1–13. https://doi.org/10.1016/j.tourman.2012.05.009

[4] Whittaker, R., McRobbie, H., Bullen, C., Rodgers, A., & Gu, Y. (2016). Mobile phone-based interventions for smoking cessation. *Cochrane Database of Systematic Reviews*, (4). https://doi.org/10.1002/14651858.CD006611.pub4

[5] Payne, T. H. (2016). The electronic health record as a catalyst for quality improvement in patient care. *Heart*, *102*(22), 1782–1787. https://doi.org/10.1136/heartjnl-2015-308724

[6] Levett-Jones, T., Hoffman, K., Dempsey, J., Jeong, S. Y. S., Noble, D., Norton, C. A., ... & Hickey, N. (2010). The 'five rights' of clinical reasoning: An educational model to enhance nursing students' ability to identify and manage clinically 'at risk'patients. *Nurse Education Today*, *30*(6), 515–520. https://doi.org/10.1016/j.nedt.2009.10.020

[7] Beauchamp, V. B., & Shafroth, P. B. (2011). Floristic composition, beta diversity, and nestedness of reference sites for restoration of xeroriparian areas. *Ecological Applications*, *21*(2), 465–476. https://doi.org/10.1890/09-1638.1

[8] U.S. Department of Health and Human Services, O. for C. R. (2023). *Annual report to Congress on breaches of unsecured protected health information for calendar year 2023*. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2023.pdf?utm_source=chatgpt.com

[9] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263

[10] Kshetri, N., & Loukoianova, E. (2019). Blockchain adoption in supply chain networks in Asia. *IT professional*, *21*(1), 11–15. https://doi.org/10.1109/MITP.2018.2881307

[11] Ryngaert, C., & Taylor, M. (2020). The GDPR as global data protection regulation? *American Journal of international Law Unbound*, *114*, 5–9. https://doi.org/10.1017/aju.2019.80

[12] Viergever, R. F., Karam, G., Reis, A., & Ghersi, D. (2014). The quality of registration of clinical trials: Still a problem. *PloS One*, *9*(1), e84727. https://doi.org/10.1371/journal.pone.0084727

[13] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). *A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data* [presentation]. Proceedings of ieee open & big data conference (vol. 13, no. 13). https://www.media.mit.edu/publications/medrec-whitepaper/

[14] Cisco. (2020). *Zero trust security: Never trust, always verify*. Cisco Systems. https://www.cisco.com/c/en/us/products/security/zero-trust.html

[15] Hall, C. M., & Ram, Y. (2020). Protecting privacy in tourism–A perspective article. *Tourism Review*, *75*(1), 76–80. https://doi.org/10.1108/TR-09-2019-0398

[16] Horowitz, M. D., Rosensweig, J. A., & Jones, C. A. (2007). Medical tourism: Globalization of the healthcare marketplace. *Medscape General Medicine*, *9*(4), 33. https://pmc.ncbi.nlm.nih.gov/articles/PMC2234298/

[17] Crooks, V. A., Kingsbury, P., Snyder, J., & Johnston, R. (2010). What is known about the patient's experience of medical tourism? A scoping review. *BMC Health Services Research*, *10*(1), 266. https://doi.org/10.1186/1472-6963-10-266

[18] Insights, Global Market. (2016). *Medical tourism market size by treatment (cosmetic treatment, dental treatment, cardiovascular treatment, orthopedic treatment, fertility treatment), by region and forecast, 2016–2025*. https://www.gminsights.com/industry-analysis/medical-tourism-market?utm_source=chatgpt.com

[19] Office of the National Coordinator for Health Information Technology. (2016). *Connecting health and care for the nation: A shared nationwide interoperability roadmap*. https://healthit.gov/topic/interoperability/connecting-health-and-care-nation-interoperability-roadmap?utm_source=chatgpt.com

[20] Detsky, A. S., Gauthier, S. R., & Fuchs, V. R. (2012). Specialization in medicine: How much is appropriate? *Jama*, *307*(5), 463–464. https://doi.org/10.1001/jama.2012.44

[21] Vest, J. R., & Gamm, L. D. (2010). Health information exchange: Persistent challenges and new strategies. *Journal of the American Medical Informatics Association: JAMIA*, *17*(3), 288. https://pmc.ncbi.nlm.nih.gov/articles/PMC2995716/

[22] Westin, A. F. (1967). *Privacy and freedom Atheneum*. Atheneum. https://openlibrary.org/books/OL5537351M/Privacy_and_freedom?utm_source=chatgpt.com

[23] Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564. https://doi.org/10.2307/40041279

[24] Katz, J. N. (2013). The three block model of universal design for learning (UDL): Engaging students in inclusive education. *Canadian Journal of Education/Revue Canadienne De L'éducation*, *36*(1), 153–194. https://cje-rce.ca/index.php/cje-rce/article/view/1159

[25] Abdelhamid, M., Gaia, J., & Sanders, G. L. (2017). Putting the focus back on the patient: How privacy concerns affect personal health information sharing intentions. *Journal of Medical Internet Research*, *19*(9), e169. https://doi.org/10.2196/jmir.6877

[26] Nurse, J. R., Creese, S., & De Roure, D. (2017). Security risk assessment in internet of things systems. *IT Professional*, *19*(5), 20–26. https://doi.org/10.1109/MITP.2017.3680959

[27] Cavoukian, A. (2012). *Privacy implications of drones: Unmanned aerial vehicles in Canada*. https://coilink.org/%0A20.500.12592/fbw15t

[28] Cavoukian, A. (2012). Privacy by design: Origins, meaning, and prospects for assuring privacy and trust in the information era. In *Privacy protection measures and technologies in business organizations: aspects and standards* (pp. 170–208). IGI Global. https://doi.org/10.4018/978-1-61350-501-4.ch007

[29] Heffner, J. L., Strawn, J. R., DelBello, M. P., Strakowski, S. M., & Anthenelli, R. M. (2011). The co-occurrence of cigarette smoking and bipolar disorder: phenomenology and treatment considerations. *Bipolar Disorders*, *13*((5-6)), 439–453. https://doi.org/10.1111/j.1399-5618.2011.00943.x

[30] Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-resistant mobile health using blockchain technology. *JMIR Mhealth and Uhealth*, *5*(7), e7938. https://doi.org/10.2196/mhealth.7938

[31] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., ... & Cardoso, M. J. (2020). The future of digital health with federated learning. *NPJ Digital Medicine*, *3*(1), 119. https://www.nature.com/articles/s41746-020-00323-1

[32] Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., ... & Prisma-P Group. (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic Reviews*, *4*(1), 1. https://doi.org/10.1186/2046-4053-4-1

[33] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *The bmj*, *372:n71*. https://doi.org/10.1136/bmj.n71

[34] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

[35] Carrera, P., & Lunt, N. (2010). A European perspective on medical tourism: the need for a knowledge base. *International Journal of Health Services*, *40*(3), 469–484. https://doi.org/10.2190/HS.40.3.e

[36] Institute, P. (2019). *Cost of a data breach report 2019*. https://insights.integrity360.com/hubfs/2019-cost-of-a-data-breach-report-04_03025203USEN.pdf?utm_source=chatgpt.com

[37] Federal Bureau of Investigation, Internet Crime Complaint Center. (2023). *Internet crime report 2023*. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf?utm_source=chatgpt.com