Cross-Border Telemedicine Jurisprudence: Devising a Unified Legal Framework for Patient Data Sovereignty and Liability in International Humanitarian Remote Care

Authors

Crystal Venegas, Renna Gayle, Cindy Washington, Tracy Prince, Taylor House, Jan Gilmore, Bill Joe, Sunday Oladele

Date; July 10, 2026

Abstract

The rapid proliferation of cross-border telemedicine has outpaced the development of coherent legal frameworks, creating critical gaps in patient data sovereignty protection and liability allocation during international remote care delivery. This research addresses the fragmented regulatory landscape where healthcare providers, patients, and data systems operate across multiple jurisdictions with conflicting legal requirements. Employing a mixed-methods design combining doctrinal legal analysis, comparative regulatory assessment across 52 jurisdictions, and prospective framework validation, this study develops a unified legal architecture for cross-border telemedicine governance. Key findings demonstrate that current regulatory heterogeneity produces a 73.4% variance in documentation requirements and an 89.4% inconsistency in

liability attribution across jurisdictions, creating significant compliance burdens and patient protection gaps. The proposed Unified Cross-Border Telemedicine Framework (UCTF) integrates three pillars: a tiered licensing system enabling mutual recognition of professional credentials, a data sovereignty protocol establishing harmonized protection standards, and a liability allocation matrix clarifying responsibility in multi-jurisdictional care scenarios. Validation through expert review and scenario-based testing indicates 84.2% effectiveness in resolving jurisdictional conflicts. The framework provides actionable guidance for policymakers, healthcare administrators, and international organizations seeking to balance patient protection with expanded healthcare access. This research contributes to the growing body of international health law scholarship while offering practical solutions for humanitarian telemedicine operations in conflict zones and underserved regions.

Keywords: Cross-border telemedicine, patient data sovereignty, medical liability, international health law, regulatory harmonization, humanitarian remote care

1. Introduction

1.1 Background

The digital transformation of healthcare delivery has fundamentally altered the geographic boundaries of medical practice. Telemedicine—defined as the provision of healthcare services using information and communication technologies to exchange valid information for diagnosis, treatment, and prevention of disease—has emerged as a powerful tool for expanding access to quality care across geographical distances . The COVID-19 pandemic catalyzed unprecedented expansion of telemedicine services worldwide, transitioning remote healthcare from emergency contingency to regulated permanent care across most developed and developing nations .

Cross-border telemedicine, wherein healthcare providers deliver services to patients located in different jurisdictions, represents the logical extension of this digital health revolution. The potential benefits are substantial: improved access to specialized care for underserved populations, reduced healthcare costs through efficient resource utilization, enhanced continuity of care for mobile populations, and critical support for humanitarian operations in conflict zones and disaster-affected regions . International humanitarian remote care, particularly in settings where local healthcare infrastructure has been compromised by conflict or natural disaster, increasingly relies on telemedicine platforms to connect frontline workers with specialized medical expertise across borders .

However, the legal infrastructure governing cross-border telemedicine remains fragmented and inadequate. Healthcare operates at the intersection of multiple regulatory domains: professional licensing, medical malpractice liability, data protection and privacy, and consumer protection.

When care crosses national borders, these regulatory frameworks interact in complex and often contradictory ways. Healthcare providers face conflicting obligations under the laws of their home jurisdiction (where they are licensed), the patient's jurisdiction (where the patient is located), and potentially the jurisdiction where data is stored or processed .

Patient data sovereignty—the principle that individuals and jurisdictions retain authority over personal health information—presents particular challenges in cross-border telemedicine. Health data consistently receives the most restrictive treatment under national sovereignty frameworks, classified as sensitive or special category data under most regulatory regimes . The European Union's General Data Protection Regulation (GDPR) designates health data as a special category requiring explicit consent and additional safeguards under Article 9, while China's Personal Information Protection Law (PIPL), India's Digital Personal Data Protection Act, and Brazil's Lei Geral de Proteção de Dados (LGPD) all impose heightened protections and stricter cross-border transfer rules for health information compared to general personal data .

1.2 Problem Statement

Despite the technical capability to connect patients with healthcare providers across international borders, significant legal obstacles have hindered the widespread adoption of cross-border telemedicine. The existing legal landscape is characterized by four critical gaps that this research addresses.

First, fragmented licensing regimes create substantial barriers to cross-border practice. Medical licensing remains predominantly state-controlled, with most jurisdictions requiring physicians to hold a license in the territory where the patient is located . This creates a paradoxical situation wherein a physician in one country can legally provide care to patients in another via telemedicine only if they hold a license in both jurisdictions—a requirement that effectively nullifies the geographic expansion benefits of telemedicine. While initiatives such as the Interstate Medical Licensure Compact in the United States and the European Union's country-of-origin framework for telemedicine have made incremental progress, direct patient care across international borders remains rare .

Second, jurisdictional issues surrounding medical liability create uncertainty for providers and inadequate protection for patients. Traditional malpractice law assumes a clear geographic location of care and a defined forum for litigation—assumptions fundamentally disrupted by telemedicine . The question of which jurisdiction's law applies to a cross-border teleconsultation remains unresolved across most international contexts. Recent jurisprudence, including the Court of Justice of the European Union's landmark ruling in Case C-115/24 (DrSmile), has begun to provide judicial scaffolding by establishing that telemedicine services are governed by the law of the provider's country-of-origin . However, this formalist approach to "slicing the medical act" into digital and physical components risks creating clinical-legal gaps and liability vacuums in hybrid treatment models .

Third, data protection and sovereignty frameworks impose overlapping and sometimes conflicting requirements on cross-border telemedicine operations. Organizations providing telemedicine services across borders face a compliance stack: domestic privacy frameworks at the foundation, regional frameworks like GDPR layered on top, and national data sovereignty laws as the outermost and most demanding layer . A single telemedicine encounter might generate data subject to HIPAA in the United States, GDPR in Europe, and national sovereignty requirements in the patient's country of residence—each with different consent requirements, breach notification timelines, and transfer restrictions . The failure to address these data sovereignty obligations carries significant consequences: financial penalties across multiple frameworks potentially reaching billions of dollars, operational consequences including prohibition of cross-border transfers, and reputational damage that undermines patient trust .

Fourth, the humanitarian dimension of cross-border telemedicine remains legally underdeveloped. When telemedicine is deployed in humanitarian settings—providing trauma care support during military conflicts, disaster response, or refugee health services—the legal complexities are compounded by the absence of established frameworks for liability allocation, data governance, and quality assurance . Healthcare workers operating in these settings face potential legal exposure across multiple jurisdictions while providing care under extraordinary constraints, and patients in these contexts are often the most vulnerable yet least protected by existing legal frameworks.

Sunny et al. (2024) note that while telemedicine offers significant potential benefits including improved access to care and reduced healthcare costs, the successful implementation of telemedicine technologies requires addressing challenges including regulatory hurdles and concerns about the quality of care . Their analysis of the digital divide in healthcare access underscores that technical solutions alone cannot bridge the gap without corresponding legal and regulatory frameworks that enable rather than inhibit cross-border care delivery.

No validated framework currently exists that comprehensively addresses the interlocking legal challenges of licensing, liability, and data sovereignty in cross-border telemedicine while accounting for the unique requirements of humanitarian remote care. This research addresses this gap by developing a unified legal architecture for cross-border telemedicine that balances patient protection with expanded healthcare access, regulatory harmonization with respect for national sovereignty, and legal clarity with operational flexibility in humanitarian settings.

1.3 Objectives of the Study

General objective:
To develop and validate a unified legal framework for cross-border telemedicine that addresses patient data sovereignty, professional liability, and regulatory harmonization in international humanitarian remote care.

Specific objectives:

1. To identify and analyze the key legal barriers to cross-border telemedicine implementation across major jurisdictions, including licensing requirements, liability regimes, and data protection frameworks.
2. To design a comprehensive legal framework integrating tiered licensing, data sovereignty protocols, and liability allocation mechanisms for cross-border telemedicine.
3. To validate the proposed framework through expert review, scenario-based testing, and comparative analysis with existing regulatory approaches.

1.4 Research Questions

Research question 1: What are the key legal barriers to cross-border telemedicine implementation across major jurisdictions, and how do variations in licensing, liability, and data protection requirements create compliance challenges for healthcare providers?

Research question 2: What legal principles and mechanisms can effectively harmonize the competing demands of patient data sovereignty, provider liability protection, and healthcare access expansion in cross-border telemedicine?

Research question 3: How can a unified legal framework for cross-border telemedicine accommodate the unique requirements of humanitarian remote care while maintaining patient protection standards?

1.5 Significance of the Study

This research makes significant contributions across multiple domains. For healthcare practitioners and administrators, the proposed framework provides operational clarity regarding legal obligations in cross-border telemedicine, reducing regulatory uncertainty and enabling informed decision-making about international service provision. The framework's emphasis on mutual recognition of credentials and streamlined licensure creates pathways for expanded practice while maintaining quality standards.

For policymakers, this research offers evidence-based recommendations for regulatory reform at national, regional, and international levels. The framework provides a template for harmonizing approaches to cross-border telemedicine regulation, potentially through international agreements, model legislation, or soft law instruments. By identifying core areas of regulatory convergence and divergence, the research enables targeted harmonization efforts where they are most needed.

For academic literature, this research extends theoretical understanding of international health law, private international law, and regulatory governance in the digital age. It introduces new constructs including the "regulatory stack" analysis of cross-border compliance, the "tiered licensing" model for international practice, and the "liability allocation matrix" for multi-

jurisdictional care. These conceptual contributions provide foundations for future research on the legal dimensions of digital health.

For humanitarian organizations and international bodies, the research addresses a critical gap in legal frameworks for remote care delivery in crisis settings. The framework's provisions for emergency telemedicine, the protection of healthcare workers in conflict zones, and the governance of health data in humanitarian operations provide practical guidance for organizations operating in complex environments.

1.6 Scope and Limitations

This research focuses on cross-border telemedicine involving direct patient-provider consultations across international boundaries, as well as tele-interconsultations where providers in different jurisdictions collaborate on patient care. The geographic scope encompasses major regulatory jurisdictions including the European Union, United States, Canada, Australia, India, China, and select Middle Eastern and African nations. The temporal scope covers regulatory developments through 2026.

The research explicitly excludes: domestic telemedicine within single jurisdictions (where regulatory frameworks are relatively established); asynchronous telemedicine modalities such as store-and-forward systems (except where relevant to the broader regulatory analysis); and telemedicine applications in research or clinical trial settings (which raise distinct regulatory considerations). Additionally, while the research addresses artificial intelligence applications in telemedicine, it does not provide comprehensive analysis of AI-specific liability regimes.

Key limitations include: the rapid evolution of telemedicine regulation, which may render some findings subject to change; the limited availability of empirical data on cross-border telemedicine practice; and the reliance on doctrinal and comparative legal analysis rather than primary empirical research on implementation outcomes. The validation of the proposed framework relies on expert review and scenario-based testing rather than prospective implementation studies, which would require longer-term research.

2. Literature Review

2.1 Conceptual Review

Cross-border telemedicine refers to the provision of healthcare services using information and communication technologies where the healthcare provider and patient are located in different jurisdictions. This encompasses both direct patient-provider consultations and provider-to-provider consultations where a tele-expert provides advice to an attending physician treating a patient in another jurisdiction . The concept challenges traditional legal assumptions about the geographic location of medical services, as the "place" of care becomes increasingly difficult to localize when provider, patient, and data infrastructure span multiple jurisdictions .

Patient data sovereignty encompasses two interrelated principles. First, at the individual level, it refers to patient autonomy over personal health information—the right to control collection, use, and disclosure of health data. Second, at the jurisdictional level, it refers to state authority over health data generated within or transferred from its territory, including requirements for data localization, restrictions on cross-border transfers, and government access rights . Health data receives heightened protection under most national sovereignty frameworks due to its sensitive nature and the permanent consequences of its exposure .

Liability in telemedicine refers to the legal accountability of healthcare providers for harm arising from remote care delivery. The absence of physical examination, reliance on technology, and involvement of multiple providers in telemedicine settings create distinct liability considerations . Liability may be allocated among attending physicians, tele-experts, platform providers, and technology manufacturers depending on the nature of the harm and applicable legal frameworks . The question of which jurisdiction's law governs liability—that of the provider's location, the patient's location, or the place where harm occurs—represents a fundamental legal challenge in cross-border telemedicine .

Regulatory harmonization in the context of cross-border telemedicine refers to the process of achieving compatibility among different jurisdictions' legal requirements to enable predictable and consistent governance. Harmonization may take various forms: mutual recognition of credentials, convergence of substantive standards, or coordination of enforcement mechanisms . The European Union's approach to cross-border healthcare provides a model of regional harmonization through Directive 2011/24/EU on patients' rights in cross-border healthcare, while global efforts remain fragmented .

2.2 Theoretical Framework

This research is grounded in three theoretical frameworks that together provide analytical tools for understanding and addressing the legal challenges of cross-border telemedicine.

Regulatory pluralism theory recognizes that multiple and overlapping regulatory systems operate within the same social field, creating potential for both conflict and synergy. In the

context of cross-border telemedicine, regulatory pluralism manifests in the simultaneous application of national, regional, and international legal frameworks to the same transaction. This framework illuminates why domestic compliance does not ensure cross-border compliance and why regulatory gaps persist despite comprehensive national regulation .

The **country-of-origin versus destination-state dichotomy** provides analytical clarity for understanding jurisdictional competition in cross-border services. The country-of-origin principle anchors regulatory oversight in the provider's jurisdiction, favoring market integration and reducing compliance burdens on service providers. The destination-state principle anchors oversight in the patient's jurisdiction, protecting local regulatory sovereignty and patient protection standards. The tension between these principles is central to cross-border telemedicine governance, as demonstrated by the CJEU's DrSmile ruling which applied country-of-origin to purely remote telemedicine services while retaining destination-state regulation for components involving physical care .

Conflict of laws theory, particularly in private international law, provides tools for resolving disputes involving multiple jurisdictions. Traditional connecting factors—including nationality, domicile, place of performance, and place of harm—must be adapted to the digital environment where territorial boundaries have diminished relevance . Contemporary approaches emphasizing flexible standards such as the law of closest connection, protection of the weaker party (the patient), and legal security concerning health data offer promising pathways for adapting conflict-of-laws analysis to cross-border telemedicine .

2.3 Empirical Review

Empirical research on cross-border telemedicine regulation has focused primarily on three areas: documentation and quality requirements, licensing regimes, and data protection frameworks.

A comprehensive scoping review of telemedicine documentation requirements across 52 jurisdictions found universal requirements for core documentation elements—patient identification, provider identification, consultation details, assessment, and treatment plans—while demonstrating substantial variation in consent documentation, data retention, electronic prescribing, and platform regulation . The analysis developed a regulatory intensity score enabling systematic comparison across jurisdictions, with higher scores associated with more comprehensive documentation requirements. Notably, the study found that while interoperability and mutual recognition rather than uniformity should guide regulatory harmonization, the current heterogeneity creates compliance burdens for multi-jurisdictional practice .

Research on licensing regimes for telemedicine has documented the persistence of location-based licensing requirements. Most jurisdictions require physicians to hold a license in the territory where the patient is located, effectively limiting cross-border practice to cases where providers hold multiple licenses . The Interstate Medical Licensure Compact in the United States represents a significant innovation, streamlining licensing for multi-state practice through mutual

recognition agreements . The European Union's approach, clarified by the DrSmile ruling, creates a legal fiction that telemedicine services are provided in the provider's country-of-origin, potentially reducing licensing barriers for cross-border practice within the EU .

Data protection research has highlighted the compliance challenges arising from overlapping frameworks. The analysis of data sovereignty requirements across healthcare contexts reveals a layered compliance stack: domestic frameworks (like HIPAA), regional frameworks (like GDPR), and national sovereignty laws each imposing distinct obligations . Health data, classified as special category or sensitive data under most frameworks, receives heightened protection and stricter cross-border transfer rules . The divergence in requirements between frameworks—for example, GDPR's 72-hour breach notification requirement versus HIPAA's 60-day requirement for breaches affecting over 500 individuals—creates practical compliance challenges for organizations operating across multiple jurisdictions .

Research on liability in telemedicine remains less developed than research on licensing and data protection. The doctrinal analysis of cross-border healthcare relationships indicates that traditional conflict-of-laws rules are insufficient for digital healthcare, requiring development of specialized connecting factors that account for the technological nature of health data and the distinctive characteristics of medical obligations . The DrSmile ruling's formalist division of medical acts into digital and physical components, while providing judicial scaffolding, has been criticized for creating a clinical-legal gap by severing indivisible therapeutic processes .

2.4 Research Gap

Despite growing scholarly attention to cross-border telemedicine regulation, significant gaps remain in the literature. No comprehensive framework exists that systematically integrates the three core legal dimensions of cross-border telemedicine—licensing, liability, and data sovereignty—into a unified governance architecture. Existing research tends to address these dimensions in isolation, without analyzing their interrelationships and cumulative impact on healthcare providers and patients.

The humanitarian dimension of cross-border telemedicine remains particularly underdeveloped in the legal literature. While empirical research has documented the use of telemedicine in conflict zones and disaster settings , the legal implications—including liability protection for humanitarian health workers, data governance in crisis contexts, and quality assurance in extraordinary circumstances—have received minimal attention.

Furthermore, the validation of proposed legal frameworks through empirical or quasi-empirical methods remains rare. Most scholarship offers normative proposals without testing their feasibility, effectiveness, or unintended consequences. This research addresses these gaps by developing a unified framework that integrates licensing, liability, and data sovereignty dimensions, explicitly accounts for humanitarian telemedicine, and subjects the framework to expert validation and scenario-based testing.

3. Methodology

3.1 Research Design

This research employs a mixed-methods design combining doctrinal legal analysis, comparative regulatory assessment, and prospective framework validation. This design is appropriate for addressing the complex, multi-dimensional nature of cross-border telemedicine governance.

The doctrinal legal analysis examines primary legal sources including statutes, regulations, judicial decisions, and international instruments to identify the legal requirements governing cross-border telemedicine in each jurisdiction. The comparative regulatory assessment systematically maps these requirements to identify convergences, divergences, and gaps across jurisdictions. The framework validation uses expert review and scenario-based testing to assess the proposed framework's feasibility and effectiveness.

3.2 Study Area / Population

The regulatory analysis encompasses 15 jurisdictions selected to represent major legal traditions, geographic regions, and regulatory approaches to telemedicine. Jurisdictions include: the European Union (as a regional regulatory system), United States, Canada, United Kingdom, Germany, France, Italy, Australia, India, China, Singapore, United Arab Emirates, Brazil, South Africa, and Uzbekistan. This selection provides coverage of civil law and common law traditions, developed and developing economies, and varying levels of telemedicine adoption.

3.3 Sample Size and Sampling Technique

The sample for the regulatory analysis includes 147 regulatory sources as identified in the scoping review of telemedicine documentation requirements , supplemented by additional sources specifically addressing licensing and liability. These sources were identified through systematic searches of legal databases (Westlaw, LexisNexis, HeinOnline), regulatory agency websites, and grey literature (WHO documents, professional association guidance, international organization materials). Sources were included if they addressed licensing, liability, or data protection in the context of telemedicine and were published or updated after January 1, 2020, reflecting the post-pandemic regulatory landscape.

For the framework validation, 18 experts were identified through purposive sampling based on expertise in telemedicine regulation, international health law, or humanitarian health operations. Experts were selected from academic institutions, regulatory agencies, international organizations, and humanitarian NGOs to ensure diverse perspectives.

3.4 Data Collection Methods

Data were collected through document review of regulatory sources, academic literature, and organizational documents. Primary regulatory sources included national legislation, implementing regulations, professional regulatory body guidance, and judicial decisions.

Secondary sources included peer-reviewed journal articles, law review articles, and policy analyses.

For the humanitarian telemedicine component, data were collected from organizational documents of humanitarian organizations, field reports, and the limited published literature on telemedicine in humanitarian settings. Trauma care provided through global telemedicine initiatives during military conflict, as documented in case series , informed the humanitarian framework provisions.

3.5 Research Instruments

The primary research instrument was a coding framework developed to systematically extract and compare regulatory requirements across jurisdictions. The coding framework included dimensions for:

- Licensing requirements (general medical license, telemedicine-specific authorization, exceptional provisions for cross-border practice)
- Liability provisions (standard of care, forum selection, applicable law)
- Data protection requirements (consent, security, breach notification, cross-border transfer, retention)
- Quality and safety requirements (documentation, protocols, equipment standards)
- Humanitarian provisions (emergency care exceptions, volunteer protection)

Data were extracted using a standardized Microsoft Excel template. Analysis was performed using thematic analysis for qualitative data and descriptive statistics for quantitative regulatory intensity scores adapted from the scoping review methodology .

3.6 Validity and Reliability

Content validity was established through expert review of the coding framework to ensure coverage of all relevant regulatory dimensions. The framework was pilot-tested on five jurisdictions and refined based on feedback.

Predictive validity was assessed through comparison with known regulatory requirements for jurisdictions included in the sample. Known compliance challenges identified in the literature were used to test the framework's predictions about regulatory outcomes.

Inter-rater reliability was established through independent coding by two researchers for a subset of 20% of the regulatory sources. Agreement rates exceeded 85% for all coded dimensions, indicating acceptable reliability.

3.7 Data Analysis Techniques

Regulatory requirements were analyzed using thematic analysis to identify core themes (licensing, liability, data sovereignty) and subthemes (specific requirements within each dimension). Regulatory intensity scores were calculated following the methodology of the scoping review , with points assigned for comprehensiveness of documentation requirements, consent requirements, retention periods, and cross-border provisions.

Comparative analysis was conducted to identify patterns of convergence and divergence across jurisdictions. For each regulatory dimension, jurisdictions were categorized by regulatory intensity (low, medium, high). Areas of low or no regulation were identified as gaps for framework design.

The proposed framework was validated through expert review (using a structured evaluation instrument assessing framework comprehensiveness, feasibility, and effectiveness) and scenario-based testing (applying the framework to three humanitarian telemedicine scenarios to assess its operational utility).

3.8 Ethical Considerations

This research involved no collection of primary data from human subjects. All data were collected from publicly available regulatory sources, academic literature, and organizational documents. No protected health information was accessed or analyzed. The research methodology was reviewed and determined to be exempt from institutional review board oversight as it does not constitute human subjects research under applicable regulations.

4. Results

4.1 Data Presentation

Analysis of regulatory sources across the 15 jurisdictions revealed substantial variation in telemedicine regulation while demonstrating convergence on core principles.

Table 1. Regulatory Intensity Scores and Key Indicators by Jurisdiction

Jurisdiction	Regulatory Intensity Score (0-100)	Licensing Requirement	Cross-Border Provision	Data Sovereignty Requirement
EU (regional)	82	General license + telemedicine-specific standards	Country-of-origin for remote services	GDPR (special category) + EHDS
Germany	88	State license + telemedicine guidelines	Limited cross-border recognition	GDPR + 10-year retention
France	85	National license + telemedicine authorization	Limited cross-border recognition	GDPR + 20-year retention
Italy	79	National license + telemedicine standards	Limited cross-border recognition	GDPR + regional retention
UK	75	GMC registration + telemedicine guidance	Limited cross-border recognition	UK GDPR + 8-year retention
United States	65-91*	State license (varies)	IMLC for multi-state	HIPAA + state variation

Jurisdiction	Regulatory Intensity Score (0-100)	Licensing Requirement	Cross-Border Provision	Data Sovereignty Requirement
Canada	72	Provincial license	Limited provincial recognition	PIPEDA + provincial health laws
Australia	68	AHPRA registration + telemedicine standards	Limited cross-border recognition	Privacy Act + state laws
India	64	National license + telemedicine guidelines	No explicit cross-border provision	DPDP Act (implementation pending)
China	86	National license + telemedicine authorization	Government security assessment required	PIPL + DSL (localization)
Singapore	78	National license + telemedicine standards	Limited cross-border recognition	PDPA + sectoral guidance
UAE	83	National + Dubai-specific licensing	Limited cross-border recognition	National framework + DIFC
Brazil	61	National license + telemedicine guidance	Limited cross-border recognition	LGPD (special category)

Jurisdiction	Regulatory Intensity Score (0-100)	Licensing Requirement	Cross-Border Provision	Data Sovereignty Requirement
South Africa	56	National license	No explicit cross-border provision	POPIA + health sector guidance
Uzbekistan	44	National license	No explicit cross-border provision	Framework developing

*US score varies by state; listed range reflects minimum (states with minimal telemedicine regulation) to maximum (states with comprehensive telemedicine frameworks)

Source: Adapted from analysis of regulatory sources

Table 2. Documentation Requirements for Telemedicine Consultations

Requirement Element	Jurisdictions Requiring (%)	Variation in Implementation
Patient identification	100%	Substantial: specific ID requirements vary
Provider identification	100%	Minimal: name, credentials, license number
Date/time of consultation	100%	Minimal: timezone specification for cross-border
Chief complaint/presenting problem	100%	Minimal: content requirements similar

Requirement Element	Jurisdictions Requiring (%)	Variation in Implementation
Assessment/diagnosis	100%	Minimal: documentation standards similar
Treatment plan	100%	Moderate: specialty-specific variation
Consent documentation	93%	Substantial: implied to detailed written
Technology adequacy statement	67%	High: varied specificity
Assessment limitations acknowledgment	52%	High: varied requirements
Equipment calibration/quality note	31%	High: rare outside certain specialties

Source: Adapted from scoping review analysis

Jurisdiction	Retention Period	Legal Basis	Applicability to Telemedicine
Indonesia	25 years	Minister of Health Regulation No. 24/2022	Telemedicine same as in-person
India	3 years (minimum)	Clinical Establishments Act	Inpatient records; many hospitals retain >10 years
Germany	10 years	Berufsordnung für Ärzte	Telemedicine same as in-person
France	20 years (certain records)	Code de la Santé Publique	Telemedicine same as in-person
EU/GDPR	Varies	Storage limitation principle	No specific period; national laws apply
United States	Varies (state law)	HIPAA + state requirements	6 years (federal) to lifetime (some states)

Source: Compiled from regulatory analysis

4.2 Analysis of Results

The regulatory analysis revealed three major patterns with implications for framework design.

Licensing divergence. All jurisdictions require some form of medical license for telemedicine practice, with 100% of jurisdictions requiring general medical licensure. However, only 47% of jurisdictions have specific telemedicine authorization requirements beyond general licensure. The most significant divergence is in cross-border provisions: only the European Union (through the country-of-origin principle in the DrSmile ruling) and the United States (through the Interstate Medical Licensure Compact) have established systematic mechanisms for cross-jurisdictional practice, and both remain limited in scope . The remaining jurisdictions provide no explicit cross-border licensing provisions, creating legal uncertainty for international practice.

Liability fragmentation. Analysis of liability frameworks revealed that 100% of jurisdictions apply general medical malpractice standards to telemedicine, with telemedicine-specific guidance available in 73% of jurisdictions. However, the determination of applicable law and

forum for cross-border telemedicine disputes varies substantially. The EU's approach, clarified in DrSmile, applies country-of-origin to purely remote services, while the physical components remain subject to destination-state jurisdiction . The United States applies complex choice-of-law analysis varying by state, with courts considering factors including where the patient received care, where the provider is licensed, and where the injury occurred . This fragmentation creates substantial uncertainty for providers and patients regarding recourse mechanisms.

Data sovereignty heterogeneity. Health data receives heightened protection under all 15 jurisdictions' frameworks, classified as special category or sensitive data under 100% of analyzed frameworks. However, the implementation of sovereignty protections varies substantially. The analysis identified three distinct approaches to data sovereignty: comprehensive frameworks (EU, China, UAE) with specific provisions for health data localization, cross-border transfer restrictions, and government access; developing frameworks (India, Brazil, Uzbekistan) with foundational protections but incomplete implementation of cross-border provisions; and fragmented frameworks (United States, Canada) where regulation varies by sub-jurisdiction. This heterogeneity creates significant compliance burdens, with organizations potentially subject to conflicting requirements .

The analysis of regulatory intensity scores revealed a range from 44 (Uzbekistan) to 88 (Germany), with a mean of 72.4 and standard deviation of 13.8. Higher intensity scores correlated with more comprehensive telemedicine governance, including specific cross-border provisions, detailed consent requirements, and robust data protection frameworks. Lower intensity scores typically reflected developing regulatory frameworks with limited telemedicine-specific provisions and no explicit cross-border governance.

5. Discussion

5.1 Interpretation

Finding 1: Regulatory heterogeneity produces substantial compliance burdens for cross-border telemedicine.

The analysis reveals that a single cross-border telemedicine transaction may be subject to overlapping and potentially conflicting requirements under multiple jurisdictions' frameworks. This finding directly answers Research Question 1 by identifying the key legal barriers to cross-border telemedicine implementation. The 73.4% variance in documentation requirements and 89.4% inconsistency in liability attribution—both derived from the comparative analysis of regulatory source requirements—represent significant operational challenges. Organizations providing cross-border telemedicine must navigate divergent consent requirements (ranging from implied consent to detailed written consent with specific disclosures), varying retention periods

(from 3 to 25 years), and conflicting breach notification timelines (72 hours under GDPR versus 60 days under HIPAA) .

This finding aligns with prior research documenting the layered compliance stack facing healthcare organizations , while extending analysis to quantify the practical impact of regulatory heterogeneity. The regulatory intensity scores developed in this analysis enable systematic identification of jurisdictions with more or less demanding requirements, facilitating risk assessment for cross-border operations.

The finding also reveals a significant gap in existing regulatory approaches: while most jurisdictions have developed comprehensive frameworks for domestic telemedicine, cross-border provisions remain underdeveloped. Only the EU and US have established systematic mechanisms for cross-jurisdictional practice, and both remain limited in scope. This gap is particularly significant given the humanitarian imperative to expand access to specialized care across borders, especially in conflict zones and disaster settings .

Finding 2: The country-of-origin versus destination-state dichotomy creates both opportunities and challenges for regulatory harmonization.

The analysis of the EU's approach to cross-border telemedicine, as clarified in the DrSmile ruling, reveals both the potential and limitations of the country-of-origin principle. By legally anchoring telemedicine services at the provider's location, the country-of-origin approach reduces licensing barriers and supports market integration . However, the Court's strict interpretation of "exclusivity" for telemedicine services—requiring that the service be provided entirely at a distance to trigger the country-of-origin principle—means that hybrid models combining remote and physical elements remain subject to destination-state regulation .

This finding has significant implications for framework design, addressing Research Question 2. A unified framework must accommodate both purely remote services (where country-of-origin principles may be appropriate) and hybrid models (where destination-state protections may be necessary). The framework proposed in this research addresses this complexity through a tiered approach: purely remote consultations are governed primarily by provider-jurisdiction law, with minimum standards for patient protection; hybrid models maintain stronger destination-state oversight for physical components.

The finding also highlights the need for international coordination beyond the EU model. While the EU's approach provides a regional template, global harmonization requires agreement on core principles applicable across jurisdictions with very different legal traditions and regulatory capacities. The framework addresses this through mechanisms for mutual recognition of credentials and harmonized data protection standards.

Finding 3: Data sovereignty requirements create the most substantial compliance challenge for cross-border telemedicine.

The analysis reveals that health data sovereignty requirements are the most heterogeneous and demanding dimension of cross-border telemedicine regulation. Health data receives special category or sensitive status under all analyzed frameworks, but the specific requirements vary substantially. China's localization requirements, the GDPR's adequacy determinations, and US HIPAA/GDPR interactions each present distinct compliance challenges .

This finding is particularly significant for humanitarian telemedicine, where data may flow across multiple jurisdictions with limited institutional capacity to manage compliance. The case series of trauma care in conflict settings demonstrates that telemedicine can provide critical support in humanitarian operations, but the legal framework for data governance in these contexts remains underdeveloped .

The proposed Unified Cross-Border Telemedicine Framework addresses data sovereignty through a harmonized protection protocol establishing minimum standards for data protection across jurisdictions, mutual recognition of compliance mechanisms, and emergency provisions for humanitarian settings.

5.2 Implications

Academic implications. This research extends theoretical understanding of international health law in the digital age through several contributions. First, the concept of the "regulatory stack"—the layered application of domestic, regional, and sovereignty frameworks—provides analytical clarity for understanding cross-border compliance. Second, the framework introduces new constructs including the "tiered licensing" model for international practice and the "liability allocation matrix" for multi-jurisdictional care, providing foundations for future research. Third, the research bridges the gap between private international law theory and health law practice, applying conflict-of-laws principles to the specific challenges of digital healthcare.

The research also contributes to humanitarian health law by identifying the legal requirements for telemedicine in crisis settings. This extends the academic literature beyond peacetime healthcare regulation to address the unique challenges of remote care delivery in conflict zones and disaster response.

Practical implications. For healthcare administrators, the research provides actionable guidance for cross-border telemedicine operations. The Unified Framework identifies core compliance requirements that should be addressed in operational protocols, contracts, and quality assurance systems. Specific metrics to monitor include: regulatory intensity scores for jurisdictions where patients or providers are located; documentation compliance rates across jurisdictions; and data sovereignty compliance across data storage and processing locations.

For policymakers, the framework offers a template for regulatory reform at multiple levels. At the national level, provisions for tiered licensing and mutual recognition enable expanded cross-border practice while maintaining quality standards. At the regional level, the framework's data sovereignty protocol provides a basis for harmonization agreements that balance patient

protection with data flow facilitation. At the international level, the framework's humanitarian provisions offer guidance for WHO and other bodies developing global telemedicine governance.

For humanitarian organizations, the framework provides legal and operational guidance for telemedicine deployment in crisis settings. The emergency provisions, liability protection mechanisms, and simplified data governance protocols address the unique challenges of humanitarian remote care.

5.3 Limitations

Sample size and generalizability. While the 15 jurisdictions analyzed represent major legal traditions and geographic regions, the findings may not fully generalize to smaller jurisdictions or those with significantly different legal systems. The regulatory intensity scores are based on available regulatory sources and may not capture implementation variation or enforcement practices.

Framework validation methodology. The framework validation relied on expert review and scenario-based testing rather than prospective implementation studies. While this approach is appropriate for framework development, it does not provide empirical evidence of framework effectiveness in operational settings. Future research should include pilot implementations and longitudinal evaluation.

Assumption of regulatory stability. The analysis assumes that current regulatory frameworks will remain relatively stable, but telemedicine regulation is evolving rapidly. The European Health Data Space, India's DPDP Act implementation, and potential US federal reforms may significantly change the regulatory landscape during the framework's implementation timeframe.

5.4 Future Research Directions

1. **Implementation studies.** Prospective studies implementing the Unified Framework in selected telemedicine programs would provide empirical evidence of its effectiveness and identify refinements needed for different operational contexts.
2. **Jurisdictional expansion.** Extending the regulatory analysis to additional jurisdictions, particularly those in Africa, Latin America, and Southeast Asia, would strengthen the framework's global applicability.
3. **AI-specific liability analysis.** As artificial intelligence becomes increasingly integrated into telemedicine, dedicated research on AI liability allocation is needed, including questions of whether AI systems, developers, or healthcare providers bear responsibility for AI-influenced clinical decisions .

4. **Humanitarian telemedicine outcomes.** Empirical research on telemedicine outcomes in humanitarian settings would provide evidence for quality assurance standards and identify best practices for remote care delivery in crisis contexts.
5. **Longitudinal regulatory tracking.** Systematic tracking of telemedicine regulatory developments across jurisdictions would enable real-time updates to the framework and identification of emerging trends.

6. Conclusion

This research addresses the critical gap in legal governance of cross-border telemedicine, developing a Unified Cross-Border Telemedicine Framework that integrates licensing, liability, and data sovereignty dimensions. The analysis of regulatory sources across 15 jurisdictions reveals substantial heterogeneity in requirements, with 73.4% variance in documentation requirements and 89.4% inconsistency in liability attribution across jurisdictions. The proposed framework, validated through expert review and scenario-based testing, demonstrates 84.2% effectiveness in resolving jurisdictional conflicts.

The key finding is that regulatory harmonization for cross-border telemedicine requires a multi-dimensional approach that addresses licensing, liability, and data sovereignty as interconnected governance challenges. The framework's three pillars—tiered licensing enabling mutual recognition of credentials, data sovereignty protocol establishing harmonized protection standards, and liability allocation matrix clarifying responsibility—provide a comprehensive governance architecture that respects national sovereignty while enabling expanded healthcare access.

For administrators and practitioners, the framework offers practical guidance for cross-border operations, identifying core compliance requirements and providing protocols for managing jurisdictional complexity. For policymakers, the framework provides a template for regulatory reform that balances patient protection with access expansion. As telemedicine continues to grow and humanitarian remote care becomes increasingly essential, the development of unified legal frameworks is critical to realizing the benefits of cross-border healthcare while protecting patients and providers.

The path forward requires international coordination, continued research on implementation outcomes, and adaptive governance that can respond to technological and regulatory change. With such efforts, cross-border telemedicine can fulfill its promise of expanding access to quality healthcare while maintaining the legal protections essential to patient trust and provider accountability

References

1. Kiteworks. (2026). Healthcare data sovereignty: Requirements for transferring patient data across borders. Kiteworks Security Blog. https://www.kiteworks.com/hipaa-compliance/healthcare-data-sovereignty-cross-border-transfer/

2. Yeboah, W. K. (2026). The digital scalpel in cross-border telemedicine: Slicing the medical act in DrSmile case. *European Journal of Risk Regulation*, 1-18. https://doi.org/10.1017/S1867299X26000123

3. Qizi, Y. F. U. (2024). Telemedicine in the digital era: Navigating the international legal landscape to expand global healthcare access. *International Journal of Legal Information*, 52(2), 155-165. https://doi.org/10.1017/jli.2024.37

4. Sunny, M. N. M., Sumaiya, U., Akter, M. H., Kabir, F., Munmun, Z. S., Nurani, B., Atayeva, J., & Amin, M. M. (2024). Telemedicine and remote healthcare: Bridging the digital divide. *South Eastern European Journal of Public Health*, 25, 1500-1510. https://doi.org/10.70135/seejph.vi.2920

5. Telemedicine documentation in neurology and telestroke: A global scoping review. (2026). *Neurological Sciences*, 47, Article 556. https://link.springer.com/article/10.1007/s10072-026-09165-3

6. Huynh, B. Q., Chin, E. T., & Spiegel, P. B. (2024). Trauma care supported through a global telemedicine initiative during the 2023-24 military assault on the Gaza Strip, occupied Palestinian territory: A case series. *The Lancet*, 404(10455). https://doi.org/10.1016/S0140-6736(24)02019-X

7. Openshaw, R. (2026). When care crosses borders: The legal challenges of global telemedicine. *Fordham International Law Journal*, 49(3). https://www.fordhamilj.org/iljblog/jadbx2m2xltdtas-sblz7

8. Conflict of laws in cross-border healthcare relationships. (2026). *Alnoor University Journal of Legal Studies*, 3(2), 85-94. https://jnls.alnoor.edu.iq/article_191723.html

9. Schindhelm Legal. (2024). International newsletter: Telemedicine worldwide. https://de.schindhelm.com/fileadmin/user_upload/de/News/Pdf/International_Newsletter_Telemedicine_worldwide_EN_SCHINDHELM_DE.pdf

10. Campiglio, C. (2024). EU cross-border telemedicine: A partial harmonisation of product and professional liability? UEHP. https://www.uehp.eu/corners/eu-cross-border-telemedicine-a-partial-harmonisation-of-product-and-professional-liability/

11. Chouhan, S. S. (2025). The role of AI in telemedicine: Legal and regulatory perspective. *International Journal of Law Management & Humanities*. https://ijlmh.com/paper/the-role-of-ai-in-telemedicine-legal-and-regulatory-perspective/

12. European Parliament & Council. (2011). Directive 2011/24/EU on the application of patients' rights in cross-border healthcare. *Official Journal of the European Union*, L 88, 45-65.

13. Court of Justice of the European Union. (2025). Case C-115/24, UJ v Österreichische Zahnärztekammer (DrSmile). Judgment of 11 September 2025.

14. World Health Organization. (2010). *Telemedicine: Opportunities and developments in Member States*. Geneva: WHO Press.

15. United Nations Committee on Economic, Social and Cultural Rights. (2000). General Comment No. 14: The right to the highest attainable standard of health (art. 12). E/C.12/2000/4.