Minnesota Journal of Business Law and Entrepreneurship

Volume 2026, No. 3

ISSN: 1540-3270

Cross-Border Telemedicine and Digital Healthcare Delivery: A Systematic Review of Licensure, Liability, Reimbursement, and Data Governance

Vivechana[1], Sushil Pal[2], Sharad Kumar[3], Archana Rani[4]

[1]College of Allied and Healthcare Sciences, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.

[2]Charak Institute of Allied and Healthcare Studies Lucknow, Uttar Pradesh, India.

[3]School of Health and Paramedical Sciences, Vivek University, Bijnor, Uttar Pradesh, India.

[4]School of Health and Paramedical Sciences, Vivek University, Bijnor, Uttar Pradesh, India.

***Corresponding author:** Vivechana,

Abstract

Cross-border telemedicine turns a clinical encounter into a multi-jurisdictional transaction. The provider, patient, payer, platform, data processor, and medical record may each be located under different legal regimes, making ordinary telehealth rules difficult to apply at scale. This systematic review and comparative legal-policy analysis examines four domains that most directly determine whether cross-border digital care can operate lawfully and sustainably: professional licensure, malpractice liability and jurisdiction, reimbursement, and health-data governance. Open-access scholarly literature published from January 2020 through August 29, 2026 was systematically searched and synthesized with current primary legal and regulatory materials from the United States, Minnesota, the European Union, India, the World Health Organization, and the World Trade Organization. Eighteen scholarly sources met the final inclusion criteria. The evidence shows that regulatory fragmentation, rather than lack of clinical technology, is the recurring constraint. U.S. interstate practice remains anchored largely to patient-location licensing, although compacts and registration pathways reduce transaction costs. Minnesota provides a notable registration pathway for out-of-state physicians and statutory private-payer telehealth parity. In the European Union, Directive 2011/24/EU, the 2025 DrSmile judgment, and the European Health Data Space create a more integrated framework, but liability, reimbursement, and hybrid-care questions remain only partly harmonized. India has a detailed domestic telemedicine framework and insurance guidance but no comparable cross-border recognition regime. The review proposes a layered compliance model that links market entry to licensure, allocates liability before care is delivered, makes payment rules portable and transparent, and treats interoperable data governance as core infrastructure rather than an ancillary privacy obligation.

Keywords Cross-border telemedicine; digital health; licensure; medical liability; reimbursement; data governance; interoperability; telehealth law; international healthcare; Minnesota Telehealth Act.

1. Introduction

Telemedicine can cross a border without the patient or clinician moving. That feature is commercially attractive because a digital service can connect scarce expertise to geographically distant patients, support continuity for mobile populations, and allow health systems or digital-health firms to serve markets beyond the location of their physical facilities. Yet the same feature destabilizes legal assumptions built around the place where care is delivered. A cross-border virtual consultation can simultaneously raise questions about who may practice medicine in the patient's location, which court and professional standard would govern an adverse event, whether a payer will reimburse the service, and whether health information may lawfully travel across the relevant jurisdictions. The World Health Organization's 2026 policy analysis identified regulatory heterogeneity, data-security and privacy constraints, financing, professional recognition, and governance as recurring barriers to cross-border telehealth.[1] The policy problem is not whether telemedicine is capable of delivering useful care. The more difficult question is whether health systems can convert technical reach into dependable legal

and economic reach. The American College of Physicians' 2026 position paper describes telemedicine as capable of improving access and reducing patient burden when it is integrated into appropriate care relationships, while also emphasizing continuing questions of payment, licensure, prescribing, equity, and safety.[2] Earlier legal analysis likewise identified state licensure, credentialing, prescribing, malpractice coverage, and protection of health information as core conditions of lawful telemedicine practice.[3] These conditions become more complex once a service is offered across state or national borders.

Licensure is the threshold market-entry rule. In the United States, the conventional approach treats the clinical service as occurring where the patient is located, which can require the physician to hold authority to practice in every state in which patients are physically present. That model protects state oversight but produces compliance costs for clinicians and firms that serve multi-state populations. Recent legal scholarship has therefore examined registration systems, compact pathways, targeted exemptions, and federal approaches as alternatives to repeated full licensure.[4] The question is not simply administrative. A licensing rule determines which market a provider can enter, how rapidly a digital-health company can scale, and whether a patient can maintain an established care relationship after crossing a state boundary.

Liability is the second boundary. Digital care does not eliminate the ordinary duty to meet the applicable standard of care, but distance can complicate diagnosis, physical examination, emergency escalation, documentation, technical failure, and informed consent. Malpractice insurance may also contain territorial or modality limits. Rowland and colleagues noted that cross-border practice can add risk where clinicians are unfamiliar with local standards or law and where technology contributes to an adverse event.[5] For hybrid services, the allocation problem becomes sharper because a remote clinician, an in-person professional, a platform, a device manufacturer, and a health system may all contribute to the same episode of care.

Payment is the third boundary. A service can be legal and clinically appropriate yet commercially nonviable if the payer treats the virtual encounter as non-covered, imposes a different rate, requires network participation that the distant provider lacks, or refuses to reimburse care furnished from another jurisdiction. Reimbursement rules also shape patient access because unclear coverage can shift costs to patients or discourage providers from offering cross-border services. Privacy and security rules form a fourth boundary. Telehealth commonly depends on video platforms, cloud infrastructure, remote monitoring devices, electronic prescriptions, and exchange of records. A systematic review of U.S. telehealth privacy and security literature identified environmental, technological, and operational risks, including data-security concerns and reimbursement or access barriers that affect the practical delivery of care.[6]

Cross-border digital health therefore operates as a linked legal system rather than four independent compliance questions. Licensure authorizes the professional act; liability rules allocate the consequences of error; reimbursement determines whether the act is economically supported; and data-governance rules determine whether the information needed for the act can be lawfully and reliably exchanged. A platform that solves only one of these domains may remain unable to deliver a stable service. This interdependence is especially visible in the European Union, where cross-border electronic prescription and patient-summary infrastructure has developed alongside health-law and data-governance rules. Empirical analysis of the eHealth Digital Service Infrastructure found growing technical capability across participating countries but comparatively limited real-world transaction volumes during the early period of operation.[7]

Interoperability is part of that legal-economic problem. A technically secure exchange can still fail if data categories, professional responsibilities, consent rules, identification methods, or legal meanings are not aligned. A 2025 scoping review of telemonitoring interoperability found heterogeneous use of standards such as HL7 FHIR, ISO/IEEE 11073, and IHE profiles, with continuing gaps in operational, organizational, and legal implementation across borders.[8] The European Health Data Space (EHDS) is intended to move the European Union toward common infrastructure and requirements, and a 2026 review concludes that it can strengthen the environment for cross-border telemedicine while leaving important legal, financial, clinical, and organizational barriers to be resolved.[9]

Reimbursement also exposes the limits of partial harmonization. Van Delm's open-access analysis of European Union cross-border digital diagnostics explains that telemedicine falls within the Patients' Rights Directive but does not fit identically within the parallel social-security coordination route, producing different reimbursement possibilities for digital and in-person cross-border care.[10] Liability is similarly incomplete. Campiglio shows that European rules provide only partial harmonization for professional and product liability when telemedicine spans national borders.[11] In 2025, the Court of Justice of the European Union addressed cross-border telemedicine directly in Case C-115/24, UJ v Österreichische Zahnärztekammer (the DrSmile case), clarifying that healthcare supplied exclusively at a distance through information and communication technology falls within the Directive's telemedicine concept and is treated as provided in the Member State where the provider is established.[12] The judgment supplies an important conflicts rule but does not convert a clinically integrated hybrid pathway into a single harmonized legal act; later commentary warns that separating remote and physical components can create new coordination and liability questions.[13]

At the global level, cross-border telehealth also sits within trade in services. Remote medical services are a form of cross-border supply under the General Agreement on Trade in Services, yet health services remain heavily shaped by domestic professional regulation, public financing, patient protection, and data law. The result is a sector in which digital delivery lowers geographic barriers more quickly than law lowers jurisdictional barriers. This gap matters to health systems, professional groups, insurers, and entrepreneurs alike because compliance architecture becomes a material component of the business model.

This article addresses that gap through a systematic review of recent open-access literature and a comparative analysis of current legal frameworks. Its principal question is: what rules and policy mechanisms most strongly influence the lawful, financially sustainable, and data-secure delivery of telemedicine across state or national borders? Four subquestions structure the analysis: (1) how do jurisdictions authorize professional practice across borders; (2) how is liability allocated when care is remote or hybrid; (3) how do reimbursement systems treat cross-border digital services; and (4) what data-governance and interoperability rules permit information to move with the patient and provider? The article then applies these findings to the United States, Minnesota, the European Union, India, and international trade and proposes a regulatory design intended to reduce unnecessary transaction costs without weakening patient protection.

1.1 Why the issue belongs in business-law and entrepreneurship scholarship

For a digital-health enterprise, cross-border compliance is not a peripheral legal function. It determines the addressable market, contracting structure, provider network, insurance requirements, data architecture, and pricing strategy. A company may have a software platform capable of serving the entire country or several countries, while its professional network is legally limited to a smaller set of jurisdictions. Each new market can require a separate analysis of professional licensing, corporate practice restrictions, telehealth consent, prescribing, payer credentialing, malpractice coverage, record retention, data processing, and consumer disclosures. Those fixed and recurring costs can favor larger incumbents over smaller firms even when both use the same underlying technology.

The business consequence is a form of regulatory fragmentation cost. A startup may respond by restricting patient eligibility according to location, using local professional entities, contracting with already licensed clinician networks, purchasing multi-jurisdictional malpractice coverage, or designing a platform around the most restrictive jurisdiction in which it operates. Each strategy changes the economics of the service. Conversely, a jurisdiction that offers a transparent registration route, predictable payment treatment, and interoperable data rules can lower entry costs without necessarily abandoning local oversight.

The patient can experience the same fragmentation as discontinuity. A university student who returns home to another state, a person who moves temporarily for work, a border-region resident, or a patient with a rare disease may be separated from an established specialist even when the technology for a follow-up consultation is readily available. Jolin and colleagues specifically identify border residents, mobile patients, and people who

need out-of-state specialty expertise as groups affected by renewed post-pandemic licensure barriers.[4] The legal issue is therefore not only market expansion; it is also the continuity and portability of lawful care.

The regulatory challenge is to distinguish protection from friction. Licensure, malpractice rules, payer review, and privacy law have legitimate protective functions. The policy objective should not be to erase them. It should be to make the rules interoperable enough that a provider can know in advance which authority governs, a patient can identify who is responsible, a payer can determine coverage without modality-based ambiguity, and health information can move through secure and standardized channels. That approach treats legal interoperability as a form of market infrastructure.

2. Methods

2.1 Review design and reporting approach

This study was designed as a systematic legal-policy review with thematic synthesis. The review followed the transparency principles of PRISMA 2020 for identification, eligibility, and reporting of scholarly evidence,[20] and the search description was informed by PRISMA-S.[21] Because the research question integrates clinical-policy literature with statutes, regulations, government guidance, and judicial decisions, a conventional meta-analysis was neither appropriate nor planned. Legal authorities were analyzed separately from the scholarly evidence and were used to determine the current law rather than to inflate the number of included academic studies.

The review period for scholarly literature was January 1, 2020 through August 29, 2026. The start date was selected to capture the rapid regulatory development associated with pandemic-era telemedicine expansion while retaining the major post-2020 scholarship on interstate and international practice. Searches were updated on August 29, 2026. Only sources with openly accessible full text, an openly accessible public-repository version, or an official public legal text were relied upon for substantive propositions in the final manuscript.

2.2 Information sources and search strategy

Scholarly searches covered PubMed/MEDLINE, PubMed Central, open-access journal repositories, and structured web discovery of publisher-hosted open-access literature. Search concepts combined telemedicine, telehealth, digital health, cross-border, interstate, international, transnational, licensure, professional recognition, malpractice, liability, jurisdiction, reimbursement, payment, privacy, cybersecurity, data governance, interoperability, electronic health records, and digital health infrastructure. Targeted backward and forward citation checking was used to identify directly relevant legal and policy scholarship not indexed consistently in biomedical databases.

A representative search logic was: (telemedicine OR telehealth OR digital health) AND (cross-border OR interstate OR international OR transnational) AND (licens* OR professional qualification OR liabilit* OR malpractice OR reimbursement OR payment OR privacy OR data governance OR interoperab*). Searches were adapted to the syntax of each source. A second stream used jurisdiction terms, including United States, Minnesota, European Union, India, and GATS, to capture comparative legal materials. The WHO 2026 cross-border telehealth policy analysis was also examined because its underlying targeted literature review and expert consultation directly addressed the same policy domains.[1]

Primary legal and regulatory materials were retrieved from official or authoritative repositories. U.S. sources included Telehealth.HHS.gov, CMS, the Interstate Medical Licensure Compact Commission, and the Minnesota Revisor of Statutes. European sources included EUR-Lex and the Court of Justice of the European Union. Indian materials included the National Medical Commission or Medical Council framework as publicly reproduced by government sources, Ministry of Health and Family Welfare materials, and the Insurance Regulatory and Development Authority of India. International trade materials were retrieved from the World Trade Organization.

2.3 Eligibility criteria

Scholarly sources were included if they met all of the following criteria: publication between January 2020 and August 29, 2026; substantive focus on telemedicine, telehealth, remote digital care, or cross-border electronic health services; direct relevance to at least one of the four prespecified domains; legal, policy, empirical, systematic-review, scoping-review, or structured implementation analysis; and availability of full text without a paywall. Sources devoted only to clinical efficacy of telemedicine without regulatory, payment, liability, data, or cross-border relevance were excluded. News articles, commercial blogs, unsourced commentary, abstracts without verifiable full text, and inaccessible closed-access articles were excluded from the evidentiary synthesis.

Eighteen scholarly sources met the final eligibility criteria and are summarized in Table 1. They include systematic and scoping reviews, legal and policy analyses, a policy position paper, an empirical cross-border digital-health infrastructure study, and a case note on the 2025 CJEU judgment. The heterogeneity of designs was expected because the research question concerns governance rather than a single clinical outcome. Accordingly, the unit of synthesis was the legal or policy proposition supported by each source, not an effect size.

2.4 Data extraction and thematic synthesis

For each included source, the review extracted jurisdiction, publication type, cross-border context, principal regulatory domain, and the finding most relevant to market entry or delivery of care. Findings were then coded into four primary domains: licensure and professional recognition; liability, jurisdiction, and standard of care; reimbursement and payment; and data governance, privacy, security, and interoperability. Cross-cutting issues such as informed consent, prescribing, quality assurance, emergency escalation, platform responsibility, and trade in services were coded as secondary themes.

The comparative legal analysis used the same four-domain matrix. A legal rule was treated as current only when it could be verified in an official source available through August 29, 2026. Where legal provisions have staged future application, the manuscript distinguishes rules already in force from rules scheduled to apply later. This is important for the EHDS, which entered into force in 2025 but applies through staged dates beginning in 2027 and later.[31]

2.5 Appraisal and limits of evidence

Formal clinical risk-of-bias tools are not well suited to statutes, legal analyses, case notes, and policy documents. The review therefore used a design-based appraisal. Greater weight was given to systematic searches, official legal texts, peer-reviewed articles with transparent methods, and analyses that directly addressed cross-border rather than ordinary domestic telehealth. Narrative commentaries were used to illuminate doctrinal or implementation questions but were not treated as proof of clinical or economic effect. Official law controlled where a scholarly source and a later primary legal authority differed.

The literature is uneven across domains. Licensure and data governance have relatively mature policy analyses, whereas cross-border malpractice outcomes and payer behavior are less often measured empirically. International comparisons also require caution because the United States, European Union, and India organize professional regulation and healthcare financing differently. The synthesis therefore identifies convergent regulatory problems while avoiding the claim that a single institutional solution can be transplanted unchanged across jurisdictions.

Table 1. Open-access scholarly evidence included in the systematic review

Source	Jurisdiction / design	Primary domain(s)	Review-relevant finding
Fields, 2020 [3]	United States; legal/regulatory review	Licensure; liability; privacy	Interstate telemedicine requires attention to state licensure, credentialing, malpractice coverage, prescribing, and protection of health information.
Dinakaran et al., 2021 [18]	India; guideline analysis	Licensure/eligibility; consent; liability; privacy	India's 2020 framework reduces ambiguity for registered practitioners but implementation still requires attention to modality, prescribing, privacy, documentation, and standard of care.
Venkatesh et al., 2022 [19]	India; policy commentary	Professional practice; consent; privacy	Describes scope and limits of the Indian Telemedicine Practice Guidelines and their importance for the governance of remote consultation.
Ftouni et al., 2022 [16]	International; systematic review	Reimbursement; privacy; implementation	Telemedicine expansion was repeatedly constrained by privacy/confidentiality, reimbursement, technology, organizational, and regulatory barriers.
Rowland et al., 2022 [5]	International/U.S.; malpractice perspective	Liability; cross-border standard of care	Cross-border telemedicine can increase malpractice complexity where local standards, technical failures, informed consent, and insurance coverage are uncertain.
Misheva & Ampovska, 2022 [17]	EU/North Macedonia; comparative legal analysis	Legal framework; professional regulation; privacy	National and regional legal variation affects telehealth implementation and underscores the need for coherent regulatory rules.
Ntafi et al., 2022 [15]	European Union; legal interoperability analysis	Data protection; transparency; liability	Legal interoperability is necessary for cross-border ePrescription and patient-summary services, not merely technical connectivity.
Bruthans & Jiráková, 2023 [7]	European Union; empirical infrastructure analysis	Data exchange; interoperability	MyHealth@EU/eHDSI capabilities expanded, but early cross-border transaction use remained concentrated and limited.

Source	Jurisdiction / design	Primary domain(s)	Review-relevant finding
Houser et al., 2023 [6]	United States; systematic review	Privacy; security; reimbursement/access	Eighteen studies showed environmental, technical, and operational privacy/security risks, including access and payer-related barriers.
Campiglio, 2024 [11]	European Union; private international law analysis	Liability; jurisdiction; applicable law	EU rules only partly harmonize professional and product liability for cross-border telemedicine.
Van Delm, 2024 [10]	European Union; open-access legal chapter	Reimbursement	Digital cross-border care can face different reimbursement pathways and constraints from comparable in-person cross-border care.
Jolin et al., 2024 [4]	United States; health-law policy analysis	Licensure; market access	Post-pandemic state licensing can interrupt interstate telehealth; registration, exemptions, and federal program-specific approaches are plausible reforms.
Martins et al., 2025 [8]	Cross-border telemonitoring; scoping review	Interoperability; standards	Twenty-five studies showed heterogeneous standards and insufficient harmonization of operational and legal implementation.
Elendu et al., 2025 [14]	International; cross-border telesurgery review	Licensure; liability; data security	Telesurgery magnifies questions of professional authority, jurisdiction, technical responsibility, informed consent, and cross-border data protection.
Carradinha et al., 2026 [9]	European Union; review	EHDS; reimbursement; data; regulation	EHDS/MyHealth@EU can support cross-border telemedicine, but legal, financial, organizational, clinical, and technical barriers persist.
Perrin Franck et al., 2026 [1]	Global; policy analysis + Delphi	All four domains	Twenty priority challenges across governance, technology, privacy, financing, quality, and resilience support coordinated international policy action.
Johnson et al., 2026 [2]	United States; professional policy position	Licensure; payment; prescribing; safety	Telemedicine can expand access, but durable integration depends on coherent payment, licensure, prescribing, and safety policy.

Source	Jurisdiction / design	Primary domain(s)	Review-relevant finding
Yeboah, 2026 [13]	European Union; CJEU case note	Jurisdiction; hybrid care; liability	DrSmile clarifies the location rule for exclusively remote care but creates coordination questions when a treatment pathway mixes remote and physical acts.

Abbreviations: CJEU, Court of Justice of the European Union; EHDS, European Health Data Space; eHDSI, eHealth Digital Service Infrastructure; EU, European Union. Table entries summarize the role of each source in this review and should not be read as equivalent levels of empirical evidence.

3. Results

3.1 Overview of the evidence

Across the eighteen included scholarly sources, the same structural problem recurred: telemedicine can be delivered across distance more easily than professional regulation, payment systems, liability rules, and health-data governance can be coordinated across jurisdictions. The WHO 2026 analysis is the clearest global expression of this convergence. Its expert process organized twenty challenges into seven domains and recommended stronger regulatory frameworks, governance, digital capacity, privacy and security, sustainable financing, and international cooperation.[1] The literature included in this review reaches a similar conclusion through different methods.

The evidence does not support a simple deregulation narrative. Licensure serves patient-protection and disciplinary functions; malpractice rules create accountability; payer rules protect benefit design and public budgets; and privacy law protects sensitive information. The problem is duplication and incompatibility. Rules that are defensible within one jurisdiction can become costly or ambiguous when applied repeatedly to a single digital service that spans several jurisdictions. This distinction is important because policy should target unnecessary friction without eliminating substantive safeguards.

The four domains also show different levels of maturity. Professional licensure is legally clear in many U.S. states but fragmented across state borders. EU telemedicine has a stronger regional conflicts rule for location of exclusively remote care, particularly after DrSmile,[12] but professional responsibility remains connected to national systems and hybrid treatment creates segmentation problems.[13] Reimbursement is comparatively predictable in jurisdictions with telehealth parity rules, such as Minnesota's private-insurance statute,[29] but cross-border payment is still constrained by payer networks, benefit design, public-program rules, and differences between national systems. Data governance is moving toward stronger regional infrastructure in the EU through the EHDS,[31] yet interoperability and cross-border transfer requirements remain operational challenges.[8,9]

3.2 Licensure and professional recognition

Licensure is the most direct legal gatekeeper for cross-border care. U.S. federal telehealth guidance describes several pathways for cross-state practice: obtaining a full license, relying on temporary practice laws, using reciprocity, participating in a compact, or registering for telehealth where a state offers that mechanism.[22] The same guidance advises providers to verify patient location before the appointment because legal authority is generally linked to where the patient is located.[22] This patient-location principle gives the receiving state a clear oversight nexus but forces multi-state providers to maintain location-aware scheduling and credentialing systems.

Interstate compacts reduce but do not erase this burden. HHS explains that compacts create faster pathways while preserving state oversight and treats the telehealth appointment as occurring in the patient's state.[23] The Interstate Medical Licensure Compact had 44 member states plus two U.S. territories and reported 65,558

physician members and 227,966 licenses issued as of July 31, 2026.[24] These figures demonstrate substantial administrative scale, but the compact remains a pathway to multiple state licenses rather than a single national medical license. The business benefit is therefore lower transaction cost and faster licensing, not complete jurisdictional unification.

The policy literature supports additional approaches. Jolin and colleagues describe targeted licensure exemptions, low-burden registration pathways, and federal program-specific rules as feasible alternatives for certain categories of care.[4] Such mechanisms are particularly relevant for follow-up visits, established patient relationships, rare-disease expertise, and mobile patients. A narrowly designed registration regime can preserve the receiving state's disciplinary jurisdiction while avoiding a full duplicative licensing process for a clinician who does not maintain a physical practice in that state.

Minnesota illustrates that model. Under Minnesota Statutes section 147.032, a physician who is not licensed in Minnesota may provide interstate telehealth to a patient located in the state if the physician holds an unrestricted license in the state from which the service is provided, has not had a license revoked or restricted, does not establish the specified physical practice presence in Minnesota, and registers annually with the Board of Medical Practice.[25] Registration subjects the physician to Minnesota law, the state judicial system, and the Board with respect to services provided to Minnesota residents.[25] The statute also creates exemptions for emergencies, irregular or infrequent services, and consultation with a Minnesota-licensed physician who retains ultimate authority.[25]

Minnesota therefore separates the right to provide remote care from the need to hold a full Minnesota medical license in defined circumstances. That is a meaningful market-entry design choice. It allows a remote clinician to serve Minnesota patients while preserving state jurisdiction over the professional relationship. The statute also requires compliance with Minnesota health-record provisions,[25] which demonstrates that licensure portability does not automatically produce data-law portability. A firm using the registration pathway must still map the other obligations that attach to the Minnesota patient.

The European Union approaches the location issue differently for cross-border healthcare within its regional legal framework. Directive 2011/24/EU provides that, for telemedicine, healthcare is considered provided in the Member State where the healthcare provider is established.[30] The 2025 DrSmile judgment confirms that the Directive's telemedicine category is limited to healthcare delivered at a distance, without simultaneous physical presence, exclusively through information and communication technology.[12] For that remote component, the country-of-origin rule creates a relatively clear location anchor. But where a treatment episode includes in-person acts in another Member State, the legal analysis can split the pathway into separate components. Yeboah argues that this formal separation may leave difficult coordination questions for clinically integrated hybrid care.[13]

India's framework is principally domestic rather than a cross-border mutual-recognition system. The Telemedicine Practice Guidelines authorize registered medical practitioners to provide telemedicine under specified professional, consent, evaluation, prescription, record, and privacy requirements.[18,19] Government materials describe the framework as addressing physician-patient relationships, liability and negligence, consent, continuity, records, privacy, security, and technology-platform considerations.[33] These rules create a substantial domestic governance base, but they do not by themselves establish a reciprocal licensing route for a physician located abroad to serve Indian patients, or for an India-registered physician to practice into another country. That international step continues to depend on the receiving jurisdiction's professional law.

3.3 Liability, jurisdiction, and the standard of care

Cross-border liability requires answers to three distinct questions: who owed a duty, which substantive standard applies, and where a claim can be brought. In ordinary teleconsultation, the clinician remains responsible for deciding whether remote assessment is appropriate, obtaining adequate information, documenting the encounter, and escalating to in-person or emergency care when needed. Fields emphasizes that telemedicine practitioners must comply with applicable licensure and credentialing rules and should verify whether malpractice coverage

extends to telemedicine and interstate practice.[3] Those practical steps matter because insurance coverage can be narrower than legal exposure.

Technology adds additional actors and causal pathways. Rowland and colleagues identify digital-health-specific malpractice risks involving diagnostic error, communication, continuity of care, technology performance, and uncertainty about customary practice.[5] In cross-border service, an adverse event may implicate the remote clinician, a local clinician, the platform, the institution that selected the technology, or a device manufacturer. The appropriate allocation depends on causation and the governing law; it should not be assumed that the platform is merely a passive conduit or that the clinician bears every technology-related failure.

Telesurgery is an extreme but informative example. Elendu and colleagues describe unresolved questions involving licensing, jurisdiction, liability allocation, consent, technical failure, and data security when a remote operator or expert participates across national borders.[14] The same questions exist in less dramatic form in tele-radiology, remote monitoring, asynchronous diagnosis, and hybrid specialty care. Where several professionals perform complementary tasks, the contract and clinical workflow should identify who retains ultimate clinical authority, who is responsible for emergency escalation, and how technical failures are managed.

European private-international-law analysis illustrates the difficulty of harmonization. Campiglio concludes that cross-border telemedicine remains only partly harmonized with respect to professional and product liability.[11] The DrSmile judgment adds clarity to the location of exclusively remote care under Directive 2011/24/EU,[12] but it does not create a comprehensive EU malpractice code. A business cannot therefore infer that provider-state treatment under the Directive eliminates all destination-state litigation, consumer, product, contractual, or professional questions. The correct approach is issue-specific and should account for the legal characterization of each component of care.

Hybrid care deserves special attention because digital business models increasingly combine remote and physical services. In DrSmile, the CJEU distinguished the remote telemedical component from healthcare that required physical presence.[12] That doctrinal distinction can be administrable from a conflicts perspective, but it can be clinically artificial if diagnosis, treatment planning, fabrication of a product, and local procedures are parts of one therapeutic episode. The risk-management response is not to rely solely on the legal label 'telemedicine.' Contracts, informed-consent materials, and professional protocols should describe responsibility at each transition point.

The liability literature also supports a principle of location transparency. A patient should be told the identity and location of the clinician, the entity responsible for the platform, how urgent problems will be handled, and which local professional will be involved if physical examination becomes necessary. The provider should know the patient's location at the time of service because that fact can determine licensing authority, emergency resources, and applicable law. HHS cross-state guidance makes patient-location verification a practical prerequisite to remote care.[22] A platform that cannot reliably determine location is therefore not only operationally weak; it may undermine the legal basis of the encounter.

Liability allocation should be prospective rather than improvised after harm. Provider agreements should address territorial malpractice coverage, indemnity, documentation, technical downtime, identity verification, local referral, emergency escalation, and responsibility for imported data. Where a platform uses automated decision support or remote devices, responsibility for alerts, thresholds, monitoring windows, and missed transmissions should be defined. These provisions do not eliminate tort duties, but they reduce ambiguity within the delivery system and can improve the evidence available if a dispute occurs.

3.4 Reimbursement and payment portability

Reimbursement is the domain in which legality and commercial viability most visibly diverge. A provider may be legally authorized to furnish telemedicine yet remain unable to bill a patient's plan, qualify for the payer's network, or receive the same rate as for in-person care. The ACP's 2026 policy paper treats payment policy as one of the central conditions for durable telemedicine integration.[2] A systematic review of pandemic-era

telemedicine challenges also identified reimbursement and financial barriers alongside technology, privacy, organizational, and regulatory problems.[16]

At the U.S. federal level, Medicare payment depends on program rules and the list of services payable under the Physician Fee Schedule when furnished through telehealth. CMS maintains a Calendar Year 2026 list of telehealth services and, under the CY 2026 Physician Fee Schedule final rule, streamlined the process for adding services and permanently removed certain visit-frequency limitations.[27,28] These changes support telehealth availability, but they do not create a general cross-state right to practice. Payment authority and professional licensure therefore remain separate compliance layers.

Minnesota creates stronger private-payer parity within its statutory scope. The Minnesota Telehealth Act requires health plans sold, issued, or renewed by a Minnesota health carrier to cover telehealth benefits in the same manner as other covered benefits and prohibits geography-based limitations subject to the enrollee's provider network.[29] It also generally requires reimbursement on the same basis and at the same rate as comparable in-person services and prohibits denial or limitation solely because the service was delivered through telehealth.[29] This is important for business planning because it reduces modality-based payment uncertainty once the service is covered and the provider satisfies network and other requirements.

Parity, however, is not the same as universal reimbursement. Minnesota's statute does not require coverage of a service that is not otherwise covered or medically necessary, and it preserves reasonable medical-management and fraud-prevention tools.[29] A provider must therefore distinguish four questions: whether telehealth is an accepted modality, whether the underlying service is a covered benefit, whether the clinician is eligible to bill or participate in the network, and whether any authorization or documentation rules apply. Treating parity as a substitute for payer contracting would overstate the law.

European cross-border reimbursement involves a different architecture. Directive 2011/24/EU allows reimbursement of qualifying cross-border healthcare up to the level of cost that would have been assumed in the Member State of affiliation if the care had been provided there, subject to entitlement and other conditions.[30] For telemedicine, the Directive treats the provider's Member State as the state of treatment.[30] Van Delm shows that digital diagnostics can nevertheless have fewer or different reimbursement options than comparable physical cross-border care because the parallel social-security coordination framework is structured around patient movement and does not map neatly onto remote care.[10] The resulting complexity can reduce the scale advantage that digital providers would otherwise obtain from serving multiple Member States.

The business implication is that payment portability should be designed alongside licensure portability. A mutual-recognition rule that lets clinicians cross borders has limited effect if reimbursement remains unavailable or requires a new network contract in every market. Conversely, a payment rule cannot authorize clinical practice. Digital-health firms need a matrix linking each payer and jurisdiction to provider authorization, network status, covered modalities, billing codes, rates, prior authorization, patient cost-sharing, and documentation. That matrix is part of the product's operating infrastructure, not merely a back-office function.

Cross-border payment also raises consumer-protection concerns. When reimbursement is uncertain, patients should receive clear information about expected coverage and potential out-of-pocket liability before care. Transparent pricing is particularly important where the provider is located in another country and the patient may have limited recourse against unexpected charges. The legal-policy literature does not support promising reimbursement merely because a service is technically available or professionally authorized.

3.5 Data governance, privacy, security, and interoperability

Cross-border telemedicine is data-intensive. A routine encounter may create identity data, scheduling information, audiovisual communications, clinical notes, prescriptions, images, laboratory results, device streams, billing data, and audit logs. These data may pass through several vendors and cloud locations before becoming part of the medical record. Houser and colleagues' systematic review demonstrates that telehealth privacy and security risk is not limited to cybersecurity; it also includes environmental privacy, technology access, workflow, and operational factors.[6] HHS guidance similarly emphasizes that telehealth information is

subject to HIPAA protections for covered entities and that providers should use technologies and workflows that protect communications and stored information.[32]

Cross-border transfer adds a conflicts layer. A provider may comply with the privacy law of the jurisdiction in which it is established while still triggering the law of the patient's jurisdiction or the rules governing an intermediary processor. In the European Union, GDPR remains central, but the policy problem is broader than consent or a lawful transfer mechanism. Clinical usefulness requires semantic and technical interoperability so that the receiving professional can understand and act on the information. Ntafi and colleagues therefore frame 'legal interoperability' as a prerequisite for cross-border eHealth services such as ePrescription and ePatientSummary.[15]

Empirical experience with European infrastructure illustrates both progress and limits. Bruthans and Jiráková found that eHDSI/MyHealth@EU capabilities expanded during 2019-2022, but real transaction use was initially concentrated, with electronic prescription between Estonia and Finland among the most mature use cases.[7] That finding is important because infrastructure availability does not guarantee adoption. Participation requires compatible national systems, workflow integration, professional trust, patient identification, translation or coding, and reimbursement incentives.

Technical standards remain fragmented. Martins and colleagues identified use of HL7 FHIR, ISO/IEEE 11073, IHE profiles, Bluetooth, REST APIs, and other approaches across telemonitoring systems, but found no fully harmonized operational model for cross-border exchange.[8] For a business, this means that compliance with a data-protection rule does not ensure that data are portable. A secure proprietary data silo can still obstruct care continuity, increase switching costs, and make international expansion expensive.

The EHDS is the most consequential current attempt to address these problems at regional scale. Regulation (EU) 2025/327 establishes MyHealth@EU as the central interoperability infrastructure for primary use of personal electronic health data and requires Member States to designate national contact points.[31] It contemplates exchange of priority categories of health data, connection of healthcare providers and pharmacies, and technical rules addressing cybersecurity, semantic interoperability, operations, and service management.[31] The Regulation also permits supplementary services that facilitate telemedicine and mobile health.[31]

The transition dates matter. The EHDS Regulation entered into force in 2025 but generally applies from March 26, 2027, with several primary-use requirements applying later to specified priority data categories beginning in 2029 and 2031.[31] It would therefore be inaccurate to describe the entire EHDS architecture as fully operational law in 2026. Firms planning EU expansion can treat the Regulation as a future-facing design constraint and investment signal, but current operations must still comply with the legal and technical rules already applicable in each Member State and under existing EU law.

Data governance should consequently be built as layered infrastructure. The first layer establishes a lawful basis and allocates controller or processor roles. The second secures identity, authentication, encryption, access control, logging, and breach response. The third addresses interoperability, data quality, coding, provenance, and clinical context. The fourth governs cross-border transfer, retention, patient access, and secondary use. The fifth defines platform responsibility for subcontractors and cloud providers. Treating only the first two layers as 'privacy compliance' leaves the clinical and commercial portability problem unsolved.

3.6 Cross-cutting finding: the four domains are sequential gates

The synthesis supports a sequential-gate model. A cross-border service must first establish professional authority to treat the patient. It must then establish the standard of care and liability architecture for the encounter. It must confirm whether payment is available and what billing conditions apply. Finally, it must ensure that the data needed to deliver, document, and continue care can move lawfully and interoperably. A failure at any gate can defeat the service even if the other three are satisfied.

The sequence is also iterative. Data architecture can affect liability because missing or unreadable records change clinical risk. Payment rules can affect data collection because billing requires specific documentation.

Licensure can affect liability because registration may submit the clinician to the receiving state's courts and professional board, as Minnesota expressly does.[25] The legal design of telemedicine should therefore be assessed at the level of the care pathway rather than through isolated compliance checklists.

4. Comparative Legal and Regulatory Analysis

4.1 United States: patient-location authority with multiple portability mechanisms

The United States has no single national civilian medical license for ordinary private telemedicine. State professional regulation remains the default, and HHS describes full licensure, temporary-practice rules, reciprocity, compacts, and telehealth registration as the main cross-state pathways.[22] This creates a layered market in which an enterprise must map each profession and state separately. Physicians may use the IMLC where available, nurses may rely on the Nurse Licensure Compact, and other professions have separate compacts or state-specific rules.[23]

This architecture has two strengths. First, it preserves the patient's state as a familiar regulator with disciplinary tools and local standards. Second, it allows experimentation: states can choose full licensing, compacts, registrations, or exemptions. The cost is fragmentation. Compliance teams must monitor patient location, license status, scope of practice, prescribing rules, consent, malpractice coverage, and payer rules across multiple legal systems. The transaction cost is highest for small firms and for services that depend on narrowly specialized clinicians.

A policy approach that respects federalism need not choose between complete state control and complete federal preemption. Jolin and colleagues outline intermediate options, including limited exemptions and streamlined registries.[4] Federal programs can also define their own portability rules within constitutional and statutory bounds. For private-sector business models, the most predictable near-term strategy is still a location-aware provider network paired with automated credentialing and payer eligibility checks.

The growth of the IMLC demonstrates demand for portability but also illustrates its legal character. As of July 31, 2026, the Compact reported 44 member states plus two U.S. territories and more than 227,000 licenses issued.[24] A platform should not treat compact participation as a substitute for maintaining state-specific licenses. It should treat the compact as a licensing accelerator and keep each destination-state authorization current.

4.2 Minnesota: registration plus payment parity as a partial interoperability model

Minnesota is particularly relevant to this journal because its statutes pair a professional entry mechanism with a comparatively strong private-payer telehealth framework. Section 147.032 allows qualifying out-of-state physicians to provide interstate telehealth to Minnesota patients through annual registration rather than full Minnesota medical licensure, subject to the statutory conditions and Minnesota's jurisdiction.[25] Section 147.033 also permits a physician-patient relationship to be established through telehealth and requires the physician to meet the same standards of practice and professional conduct that apply to in-person care.[26]

The combination is notable. Registration lowers one barrier to market entry, but it does not lower the substantive standard of care. By agreeing to Minnesota law and the state's judicial and disciplinary systems, the remote physician accepts the receiving state's accountability structure.[25] This is a useful template for portability because it separates the administrative burden of full licensure from the state's interest in quality and discipline.

The Minnesota Telehealth Act then addresses payer treatment. It requires covered health plans to cover benefits delivered through telehealth in the same manner as other benefits, restricts geography-based limitations subject to the plan's network, applies comparable cost-sharing rules, and generally requires reimbursement on the same basis and at the same rate as in-person services.[29] The statute also requires telehealth technology to satisfy current industry interoperable standards and applicable HIPAA standards in the relevant provision.[29] Professional authority, payment parity, and technology standards are therefore linked in one state policy environment, although they remain separate statutes and obligations.

For digital-health enterprises, the Minnesota model suggests a practical compliance sequence: register eligible out-of-state clinicians; verify that each encounter falls within the registration pathway; submit to Minnesota professional and record rules; contract with payers or satisfy their network requirements; and use technology that meets interoperability and privacy requirements. The model does not eliminate every barrier, but it demonstrates that a state can reduce licensing friction while preserving local accountability and a stable payment rule.

There are also limits. Section 147.032 applies to physicians and has defined conditions and exemptions; it should not be generalized automatically to every health profession.[25] The Telehealth Act does not force a plan to cover services that are not otherwise included or medically necessary.[29] Nor does payment parity by itself create interstate provider-network participation. These limits reinforce the broader finding that cross-border digital care depends on coordinated, not merely generous, rules.

4.3 European Union: country-of-origin telemedicine, cross-border reimbursement, and the EHDS transition

The European Union has a more explicit supranational framework for cross-border healthcare. Directive 2011/24/EU defines cross-border healthcare and provides that, for telemedicine, care is considered provided in the Member State where the provider is established.[30] It also creates patient reimbursement rights subject to the benefit package and reimbursement level of the Member State of affiliation.[30] This framework gives digital providers a conflicts rule that the U.S. state system lacks, but it does not fully harmonize professional liability, national benefit design, or health-system organization.

DrSmile is now central to understanding the Directive. The CJEU held on September 11, 2025 that telemedicine, for the relevant provisions, corresponds to healthcare supplied at a distance and exclusively by information and communication technology.[12] The country-of-origin treatment rule applies to that remote component. In a complex pathway that includes physical healthcare, however, the physical acts retain their own territorial character. The judgment therefore makes the legal unit of analysis smaller than the entire commercial treatment package.

That segmentation has practical consequences. A cross-border dental, dermatology, fertility, diagnostic, or remote-monitoring business may sell one integrated service while the law characterizes different components separately. Yeboah argues that this can create a clinical-legal gap in hybrid models because the therapeutic process may be integrated even when the legal acts are divided.[13] Contracting should therefore identify which entity and professional performs each component, the governing professional rules, how responsibility passes between remote and local actors, and how the patient can complain or seek redress.

Reimbursement remains differentiated. Under Directive 2011/24/EU, the Member State of affiliation determines the healthcare for which the insured person is entitled to assumption of costs and generally reimburses cross-border care up to the domestic level, without exceeding the actual cost.[30] Van Delm explains that telemedicine does not fit equally within the parallel social-security coordination framework, which can leave digital cross-border care with a narrower or less intuitive reimbursement route than in-person care.[10] This illustrates a general point: a single-market rule for service location does not automatically create a single market for health insurance reimbursement.

Data infrastructure is where EU integration is advancing most visibly. The EHDS establishes MyHealth@EU and requires national contact points and cross-border data exchange infrastructure.[31] It aims to make patient summaries, ePrescriptions and dispensations, imaging, test results, discharge reports, and other priority categories increasingly portable through common formats and staged implementation.[31] Carradinha and colleagues conclude that the framework can improve trust and scalability for cross-border telemedicine, but legal, financial, technical, and organizational barriers remain.[9]

The staged application dates require careful compliance planning. The Regulation generally applies from March 26, 2027, while several primary-use obligations apply to priority categories later, including 2029 and 2031 dates.[31] Firms should therefore distinguish 'designing for EHDS' from 'claiming EHDS compliance' before an

obligation applies. Premature claims can mislead customers and investors; delayed preparation can create expensive re-engineering when common formats and connection requirements become mandatory.

Overall, the EU model is moving toward regional legal and technical interoperability without fully displacing national health systems. The country-of-origin rule for exclusively remote care reduces some jurisdictional uncertainty. The Directive creates a reimbursement framework, the CJEU has clarified the telemedicine concept, and EHDS builds common data infrastructure. Yet professional liability, hybrid treatment, benefit design, and implementation remain areas in which national differences continue to matter.

4.4 India: detailed domestic telemedicine governance with limited international portability

India's 2020 Telemedicine Practice Guidelines created a detailed domestic framework for registered medical practitioners. The framework addresses identification, consent, appropriateness of telemedicine, patient evaluation, medication categories, documentation, privacy, and professional responsibilities.[18,19] Government descriptions also emphasize physician-patient relationships, liability and negligence, continuity, medical records, privacy and security, and technology platforms.[33] This level of domestic detail is valuable because it reduces uncertainty about how a teleconsultation should be conducted.

The Insurance Regulatory and Development Authority of India complemented the professional framework by advising health insurers to allow telemedicine wherever consultation with a medical practitioner is covered under the policy, subject to the policy's sublimits and other terms.[34] This is a useful example of aligning payment with professional authorization. It does not create universal parity in the Minnesota sense, but it reduces the risk that telemedicine will be excluded solely because the consultation occurs remotely where the policy otherwise covers consultation.

For cross-border practice, however, the framework remains asymmetric. The Indian rules authorize eligible Indian practitioners under Indian law; they do not create a treaty-based or reciprocal right to practice medicine into another country, nor a general route for foreign clinicians to treat Indian patients without satisfying Indian professional law. A digital-health company that exports consultation services from India must therefore analyze the destination country's licensing and liability rules. A foreign platform entering India must analyze Indian professional, data, prescription, consumer, and insurance requirements. The domestic telemedicine guidelines are a foundation, not an international passport.

This distinction matters for India's potential role as an exporter of digital health expertise. Cross-border supply can expand access and create economic opportunity, but professional services are heavily regulated because states retain legitimate interests in competence, discipline, safety, and patient redress. International scaling is therefore more likely to depend on bilateral recognition, institution-to-institution tele-expertise arrangements, locally licensed professional networks, or narrowly defined consultation models than on unilateral domestic guidelines alone.

4.5 International trade and global governance

The World Trade Organization classifies remote delivery of services across a border as Mode 1 cross-border supply under the GATS framework. Its health-services materials specifically note that telemedicine increases the importance of Mode 1, while also observing that commitments for this mode are comparatively limited.[35] This helps explain why technical capability does not automatically produce legal market access. Domestic regulation of health professionals, data, and public financing can remain decisive even where a service is digitally tradable.

The WHO 2026 analysis approaches the same problem from a health-system perspective rather than a trade-law perspective. It recommends interoperable regulatory frameworks, stronger coordination, data protection, sustainable financing, capacity building, and reduction of unnecessary barriers.[1] The convergence of trade and health-policy analysis is significant. Cross-border telemedicine is neither an ordinary e-commerce service nor a purely local medical act. It is a regulated professional service delivered through digital infrastructure, often financed by public or quasi-public systems and dependent on sensitive-data exchange.

Global governance should therefore focus on minimum compatibility rather than complete legal uniformity. Countries need not adopt identical standards of care, liability rules, or benefit packages to make cross-border telemedicine more workable. They can instead agree on recognition criteria, identity and credential verification, minimum professional disclosures, secure transfer standards, complaint pathways, malpractice coverage, and rules for emergency escalation. Such arrangements are closer to interoperability protocols than to wholesale harmonization.

Table 2. Comparative legal architecture for cross-border telemedicine

Jurisdiction	Licensure / market entry	Liability anchor	Reimbursement	Data governance / interoperability
United States	Patient-location licensing is the default; full licenses, temporary rules, reciprocity, compacts, and registrations may be available.[22,23]	State professional/tort law; territorial malpractice coverage and standard-of-care issues remain important.[3,5]	Medicare and private-payer rules vary; payment does not itself authorize interstate practice.[27,28]	HIPAA plus state law; vendor, security, record, and interoperability obligations depend on service and actors.[32]
Minnesota	Qualifying out-of-state physicians may use annual interstate telehealth registration under §147.032.[25]	Registrant submits to Minnesota law, courts, and Board; telehealth standard remains equivalent to professional expectations.[25,26]	Private-plan coverage and reimbursement parity within statutory scope; network and coverage conditions remain.[29]	Minnesota records law applies to interstate physicians; Telehealth Act references interoperable industry standards and HIPAA.[25,29]
European Union	Directive treats exclusively remote telemedicine as provided where provider is established; DrSmile clarifies remote vs physical components.[12,30]	Only partial harmonization; hybrid pathways can engage multiple legal regimes.[11,13]	Directive 2011/24 reimbursement depends on entitlement and home-state level; digital care does not map identically to all social-security routes.[10,30]	GDPR plus evolving EHDS/MyHealth@EU infrastructure; staged application begins 2027 with later dates for key primary-use obligations.[31]
India	2020 Telemedicine Practice Guidelines authorize registered practitioners domestically; no general international mutual-recognition regime.[18,19,33]	Professional negligence, consent, documentation, prescribing, privacy, and platform duties remain within Indian legal framework.[18,33]	IRDAI advises telemedicine coverage where consultation is covered under policy terms.[34]	Guidelines address privacy/security and digital records; cross-border transfer requires separate legal analysis.[18,19]

Jurisdiction	Licensure / market entry	Liability anchor	Reimbursement	Data governance / interoperability
International trade	Telemedicine is potentially GATS Mode 1 cross-border supply, subject to domestic regulatory commitments and limitations.[35]	No global malpractice code; jurisdiction and redress remain national or contractual.	No global reimbursement portability; payer and national benefit systems dominate.	WHO calls for interoperable privacy, governance, and operational frameworks rather than purely technical connectivity.[1]

5. Discussion

5.1 Cross-border telemedicine is an interoperability problem in law as well as technology

The central finding of this review is that cross-border telemedicine is best understood as a legal interoperability problem. A technology platform can connect a clinician and patient instantly, but a lawful care pathway also requires compatible rules for professional authority, responsibility, payment, and data movement. Existing policy often treats these issues separately because they are administered by different institutions: medical boards regulate professionals, courts and insurers shape liability, public agencies and private payers determine reimbursement, and privacy or digital-health regulators govern data. Digital delivery exposes the cost of that institutional separation.

The evidence suggests that complete harmonization is neither realistic nor necessary. The United States is unlikely to replace state medical regulation rapidly with a national civilian license. EU Member States retain significant competence over health-system organization and benefits. India has its own professional framework and financing structure. A workable model can instead make the interfaces predictable. Mutual recognition or streamlined registration can standardize market entry; choice-of-law and responsibility rules can clarify liability; benefit and network rules can be made transparent; and data can move through common standards with defined controller responsibilities.

Minnesota demonstrates one version of this approach. An out-of-state physician can use a registration pathway while accepting Minnesota's jurisdiction and record rules.[25] The state separately requires strong private-payer telehealth parity.[29] This is not full interoperability, but it aligns two important gates: market entry and payment. The EU demonstrates another version: the Directive anchors remote treatment in the provider's state,[30] while the EHDS builds common data infrastructure.[31] Each model solves a different part of the same problem.

The distinction between administrative portability and substantive accountability should guide reform. Lowering paperwork should not lower the standard of care. Minnesota's framework shows that a state can permit remote entry while retaining disciplinary and judicial authority.[25,26] Similarly, compacts can accelerate licensing while preserving destination-state oversight.[23] The business-law objective is therefore not deregulation but reduction of duplicative process where substantive protections can be maintained through recognition, registration, shared data, and reciprocal enforcement.

5.2 The patient-location rule and the provider-location rule reflect different regulatory choices

The contrast between the U.S. and EU location rules is conceptually important. U.S. practice generally uses patient location as the licensing anchor.[22] This prioritizes the receiving jurisdiction's power to protect residents. Directive 2011/24/EU, by contrast, deems telemedicine provided in the Member State where the provider is established.[30] This facilitates cross-border service supply within a supranational legal framework that already includes rules on professional qualifications, free movement, patient rights, and data protection.

Neither rule is universally superior. A patient-location rule makes local redress and professional control easier to understand but creates a licensing mosaic. A provider-location rule can support scale but depends on trust that the provider's home jurisdiction maintains adequate professional oversight and that patient remedies remain effective. The EU can rely on a degree of common legal infrastructure that does not exist among unrelated countries. Global policy should therefore avoid assuming that the EU country-of-origin rule can be copied without the institutional conditions that support it.

A hybrid approach is plausible for interstate U.S. telemedicine. States could retain patient-state jurisdiction over complaints and substantive patient-protection rules while accepting an out-of-state license through low-burden registration for defined remote services. Minnesota already approximates this structure for physicians.[25] Expansion of such arrangements could be tied to continuous license verification, malpractice coverage, data-sharing for disciplinary actions, and an express consent to the destination state's jurisdiction.

5.3 Liability should follow functions, not platform labels

The literature does not support a single liability rule for all telemedicine. A video follow-up, asynchronous image review, remote intensive-care consultation, robotic telesurgery, and algorithm-supported monitoring create different risk structures. The correct question is which actor controlled the relevant function. The clinician controls diagnosis and treatment decisions; a local provider may control physical examination or procedure; a platform may control communication reliability and identity tools; a device manufacturer may control hardware performance; and an institution may control credentialing or staffing.

Function-based allocation is especially important after DrSmile. The CJEU's distinction between exclusively remote telemedicine and physical care may lead legal analysis to segment a service that a company sells as one package.[12,13] Contracts should reflect that segmentation before the patient enters the pathway. A master services agreement between remote and local providers should not merely say that each party is responsible for its own acts. It should define handoffs, decision authority, availability, escalation, record access, device responsibility, and patient communications.

Insurance should mirror the same map. A clinician's malpractice policy should cover the jurisdictions and modalities in which care is delivered. Platform cyber coverage is not a substitute for professional liability, and professional liability may not cover a platform's contractual or data-security failure. Telesurgery and remote monitoring make these distinctions visible,[14] but the same principle applies to ordinary digital care.

5.4 Reimbursement is a regulatory incentive, not merely a billing detail

Payment policy determines whether a legally available modality becomes routine. Temporary pandemic expansion showed that utilization can change rapidly when payment and regulatory barriers are relaxed; the 2026 ACP position paper treats durable payment policy as essential to responsible integration.[2] When reimbursement remains uncertain, providers have less incentive to invest in infrastructure, credentialing, and cross-border compliance. Patients may also be exposed to unpredictable self-pay charges.

Parity rules can reduce modality discrimination, but they require careful drafting. Minnesota's same-basis and same-rate provisions provide predictability within the private health-plan context,[29] yet the statute preserves medical necessity, benefit design, network, and reasonable management rules. This balance avoids the stronger and less defensible claim that every remote service must be paid regardless of clinical appropriateness or coverage. For cross-border policy, a similar distinction should separate modality neutrality from universal coverage.

International reimbursement is harder because national health systems differ in benefits, tariffs, gatekeeping, and public financing. Directive 2011/24/EU provides a common legal route but leaves the Member State of affiliation to determine entitlement and reimbursement level.[30] Van Delm's analysis shows why digital care can still be disadvantaged when reimbursement law assumes physical travel.[10] As health services become more digital, financing rules will need to define what constitutes the place and unit of service without using physical presence as an unexamined proxy.

5.5 Data portability should be treated as continuity-of-care infrastructure

Privacy regulation is often discussed as a restriction on data use, but cross-border telemedicine also requires a positive law of data availability. A clinician cannot safely treat a patient if clinically important information is inaccessible, untranslated, or trapped in an incompatible system. Ntafi and colleagues' concept of legal interoperability captures this point: rules must permit and give meaning to exchange, not merely prevent unauthorized disclosure.[15]

The EHDS moves in this direction by making MyHealth@EU a mandatory infrastructure and defining common exchange responsibilities.[31] Its staged implementation is a reminder that technical interoperability is costly and institutionally complex. The early eHDSI experience showed that even when cross-border services exist, use can remain limited.[7] Policy should therefore measure real transactions, successful record retrieval, medication reconciliation, patient understanding, and clinical use rather than treating connection to a network as the endpoint.

For businesses, interoperability can reduce long-run compliance and integration costs. Common formats reduce the need to build bespoke interfaces for every partner or country. At the same time, standardization can impose short-run engineering costs and require changes to legacy systems. The predictable announcement of transition dates, such as those in the EHDS,[31] allows firms to schedule those investments and can reduce regulatory surprise.

5.6 Equity and competition considerations

Cross-border telemedicine can improve access to specialists, but regulatory reform can distribute benefits unevenly. Large platforms may be better positioned than independent clinicians to maintain multiple licenses, payer contracts, security programs, and data integrations. Excessive jurisdiction-by-jurisdiction compliance can therefore operate as a barrier to entry. Streamlined registration and common data standards may increase competition by lowering fixed costs, provided patient-protection obligations remain enforceable.

Digital access also matters. Privacy, security, and interoperability reforms do little for patients who lack reliable connectivity, appropriate devices, language support, digital literacy, or private space. The systematic review by Houser and colleagues identifies environmental and access dimensions of telehealth privacy and security,[6] and the WHO framework includes digital capacity and awareness among the cross-border policy challenges.[1] A sustainable regulatory model should therefore avoid defining success solely as the number of jurisdictions a platform can enter.

There is also a risk of regulatory arbitrage. A provider-location rule can create incentives to establish operations in a jurisdiction perceived as less burdensome. A patient-location rule can create incentives to block patients in strict jurisdictions. Neither response is desirable if it undermines access or quality. Mutual recognition should therefore depend on minimum professional standards, reciprocal disciplinary information, adequate malpractice coverage, and transparent patient remedies.

6. A Regulatory Design for Cross-Border Digital Healthcare

6.1 Principle 1: establish a portable but accountable professional authorization

The first reform is a portable authorization that is lighter than repeated full licensure but stronger than unregulated practice. For interstate U.S. physicians, this can take the form of an expanded compact or Minnesota-style registration. The receiving jurisdiction should be able to verify the home license electronically, receive notice of disciplinary action, require malpractice coverage, enforce its standard of care for local patients where appropriate, and exercise disciplinary jurisdiction over services delivered to its residents. The clinician should not need to create a physical office or complete duplicative training merely because the consultation is remote.

For international arrangements, mutual recognition is more difficult and should be limited to jurisdictions with comparable professional standards and reciprocal enforcement. A bilateral or regional agreement could identify

eligible professions, minimum qualification standards, disciplinary-data exchange, language competence where relevant, scope limitations, prescribing rules, and emergency obligations. The WHO's recommendation for interoperable regulatory frameworks supports this direction without requiring full harmonization.[1]

6.2 Principle 2: create a pre-care liability matrix

Every cross-border service should maintain a written liability matrix before care is offered. The matrix should identify the remote clinician, local clinician if any, clinical entity, technology vendor, device supplier, and payer-facing entity. For each actor it should state the function controlled, governing contract, professional or commercial insurance, record obligations, escalation responsibilities, and dispute or complaint pathway. The patient-facing disclosure should be simpler but should identify the responsible clinician and how urgent or in-person care will be arranged.

This approach is particularly important for hybrid models after DrSmile.[12,13] A company should not rely on a single consumer brand to imply a single legal actor if the underlying treatment is divided among entities and jurisdictions. Clear role allocation can reduce gaps in informed consent, prevent duplicated or omitted tasks, and make insurance procurement more accurate.

6.3 Principle 3: make reimbursement rules portable, transparent, and modality-neutral where clinically appropriate

Payers should state whether a covered service remains covered when delivered through an approved telemedicine modality and whether cross-border provider status changes eligibility. Where the underlying service is clinically appropriate for telemedicine, reimbursement policy should avoid arbitrary denial based solely on the remote modality. Minnesota's statute provides a strong example of modality parity while preserving coverage and medical-management conditions.[29]

For public programs and international systems, portability may require separate agreements. A regional rule could define how the home payer verifies provider authorization, which tariff applies, whether prior authorization is required, and how fraud or duplicate billing is controlled. The EU experience shows that reimbursement rules designed around patient travel should be re-examined when the patient remains at home and only the service crosses the border.[10,30]

6.4 Principle 4: treat data portability as a regulated utility layer

Cross-border data exchange should use defined identity, authentication, coding, interoperability, security, and audit standards. The legal framework should specify controller or processor roles, breach responsibility, transfer mechanisms, patient access, and retention. Technical standards should be selected to support clinical use rather than simply satisfy transmission requirements. The EHDS model is instructive because MyHealth@EU combines interoperability, security, national contact points, and defined categories of health data within one architecture.[31]

Where a regional infrastructure does not exist, contractual interoperability can provide an interim mechanism. Provider networks can agree on a minimum patient summary, medication list, allergies, diagnoses, recent results, provenance metadata, and emergency contact information. This will not create the full functionality of a public exchange, but it can reduce clinical risk and vendor lock-in.

6.5 Principle 5: require location-aware compliance by design

Because legal obligations often turn on patient location, location awareness should be embedded in the service workflow. Before each encounter, the platform should confirm the patient's physical location, verify that the clinician is authorized for that jurisdiction, display relevant consent or emergency information, check prescribing restrictions, and ensure that the selected payer workflow is available. This is a form of regulatory technology rather than surveillance: the system needs the jurisdictional fact necessary to determine whether it may lawfully proceed.

Location logic should also handle uncertainty. If the patient is traveling, the platform should not assume that the address on file controls. If a clinician loses authorization in a jurisdiction, future appointments should be blocked or reassigned. If a local emergency resource is required, the platform should display information appropriate to the patient's actual location. These controls convert compliance from a periodic legal review into an operational safeguard.

6.6 Principle 6: build staged pathways for low-risk continuity care and higher-risk interventions

Not every telemedicine service requires the same portability rule. Lower-risk continuity visits with an established patient may justify broader registration or exemption than first-contact prescribing, complex diagnosis without local examination, or telesurgery. Risk-tiered regulation can reduce unnecessary burdens while preserving stricter requirements where remote limitations have greater clinical consequences. Jolin and colleagues specifically discuss exemptions for follow-up care as one potential U.S. reform.[4]

A tiered framework could distinguish: established-patient follow-up; specialist tele-expertise to a local clinician; direct-to-patient first consultation; remote prescribing of higher-risk medications; continuous remote monitoring; and remote procedural assistance or telesurgery. Each tier could specify licensing, consent, local backup, insurance, data, and quality requirements. This is more defensible than treating every video-enabled service as legally identical.

6.7 Principle 7: publish measurable indicators of cross-border performance

Regulators and health systems should evaluate whether portability actually improves care. Useful indicators include number of cross-border encounters, specialties involved, wait-time reduction, continuity for mobile patients, claim-denial rates, patient out-of-pocket costs, adverse-event and complaint rates, data-exchange success, emergency transfers, and disciplinary actions. The early MyHealth@EU experience demonstrates why measuring actual transactions matters; capability alone can overstate practical adoption.[7]

Business reporting should similarly distinguish registered markets from active markets. A platform that holds licenses or registrations in many jurisdictions but has limited payer access, sparse clinician coverage, or poor data integration does not have the same operational reach as one that can complete end-to-end care. Clear metrics reduce the risk that regulatory permissions are presented as equivalent to mature service capacity.

Table 3. Proposed cross-border telemedicine compliance architecture

Gate	Minimum precondition	Operational control	Failure if omitted
1. Professional authority	Provider holds license, compact privilege, registration, exemption, or recognized authorization for patient location.	Real-time credential and patient-location verification.	Unauthorized practice; disciplinary exposure; invalid billing or contracts.
2. Clinical suitability	Remote modality is appropriate for the condition and patient.	Triage rules; escalation to local/in-person care; emergency workflow.	Diagnostic delay; unsafe remote management; malpractice risk.
3. Liability allocation	Applicable professional standards and actor responsibilities are identified.	Territorial malpractice coverage; role matrix; handoff documentation.	Coverage gaps; fragmented responsibility; avoidable litigation uncertainty.

Gate	Minimum precondition	Operational control	Failure if omitted
4. Payment eligibility	Underlying service is covered and provider is eligible for relevant payer/network.	Payer-specific eligibility, authorization, coding, and cost estimate.	Denied claims; unexpected patient charges; unsustainable service line.
5. Data-law authority	Lawful collection, processing, storage, and transfer basis exists.	Controller/processor map; contracts; access control; retention; breach plan.	Privacy violations; transfer restrictions; contractual liability.
6. Interoperability	Clinical data can be understood and used by receiving professionals.	Common formats, coding, provenance, patient summary, audit trail.	Data silos; duplicate testing; unsafe transitions; high integration costs.
7. Patient transparency	Patient knows provider identity/location, limits of remote care, payment exposure, and complaint route.	Jurisdiction-specific disclosures and consent.	Inadequate consent; consumer-protection risk; loss of trust.
8. Ongoing monitoring	Regulatory and operational conditions remain valid after launch.	License alerts, policy updates, payer changes, security audits, quality metrics.	Silent noncompliance as law, credentials, or coverage changes.

7. Implications for Digital-Health Enterprises, Health Systems, and Policymakers

7.1 Digital-health enterprises

A company planning cross-border expansion should begin with a jurisdictional map rather than a marketing map. The relevant unit is not simply the country or state in which demand exists. It is the combination of patient location, professional authorization, clinical service, payer, data flow, and local backup. Expansion should be sequenced toward jurisdictions in which these elements can be satisfied together. Entering a market merely because a clinician can be licensed there may produce an unusable market if reimbursement or data access remains absent.

Compliance architecture should also be reflected in product design. Scheduling should be location-aware; clinician profiles should connect to credential databases; consent should change when the applicable jurisdiction changes; clinical workflows should contain escalation triggers; billing should validate payer requirements; and the data layer should support export in common formats. Legal advice remains necessary, but a scalable service cannot depend on a lawyer manually approving every routine encounter.

Contracts should be modular. Provider agreements, platform terms, data-processing agreements, payer contracts, vendor agreements, and local referral arrangements should use consistent definitions of the service and responsibilities. A mismatch—for example, a clinical agreement that treats a local physician as the final decision-maker while the patient-facing platform portrays the remote specialist as solely responsible—creates avoidable risk.

7.2 Health systems and professional groups

Health systems can use cross-border telemedicine to extend specialty expertise without creating a full physical presence in every market, but governance should remain clinically integrated. Credentialing, quality review, incident reporting, and medical-record access should include remote clinicians. Tele-expertise models in which a remote specialist advises a locally responsible clinician may reduce some direct-to-patient licensing and emergency concerns, although the legal characterization must still be verified in each jurisdiction.

Professional groups should view portability as compatible with professional standards. Compact or registration systems can require an unrestricted home license, discipline reporting, continuing competence, insurance, and consent to receiving-state jurisdiction. This can preserve the profession's regulatory role while reducing duplication. The IMLC's scale indicates that clinicians and boards already use such administrative cooperation extensively.[24]

7.3 Policymakers

Policymakers should evaluate cross-border telemedicine through the combined effect of rules rather than one statute at a time. A state may liberalize licensing but retain payment rules that make service uneconomic. A country may enable reimbursement but prohibit data transfer needed for clinical records. A region may create data infrastructure without resolving professional liability. Regulatory-impact analysis should therefore trace a complete encounter from patient onboarding to follow-up and claims payment.

New rules should also contain transition periods and technical implementation guidance. The EHDS demonstrates the value of announcing staged dates for a complex data architecture.[31] Similar predictability would help providers adapt to new credentialing, security, or payment requirements. Sudden changes can disrupt established patient relationships even when the policy goal is legitimate.

Finally, policymakers should preserve local accountability. Cross-border care should not create a zone in which patients cannot identify a regulator, obtain records, file a complaint, or enforce a judgment. Portability is sustainable only when it is paired with a clear responsible professional, enforceable jurisdiction, adequate insurance, and transparent redress.

8. Limitations

This review has several limitations. First, the scholarly evidence is methodologically heterogeneous. It includes systematic and scoping reviews, policy analysis, legal scholarship, empirical infrastructure analysis, professional guidance, and case commentary. This heterogeneity is appropriate to the interdisciplinary research question but prevents quantitative pooling and means that the conclusions concern regulatory structure rather than pooled clinical outcomes.

Second, the open-access criterion was intentionally strict because the manuscript was designed to rely on sources that readers can verify without subscription access. That choice improves transparency but may exclude relevant closed-access scholarship. The principal legal propositions were therefore cross-checked against statutes, regulations, official government guidance, and judicial decisions so that the omission of a closed-access commentary would not determine the statement of current law.

Third, telemedicine law changes rapidly. The review and primary legal materials are current through August 29, 2026, but licensing statutes, compact membership, payer rules, federal telehealth policies, and EHDS implementation measures may change. The EHDS in particular has staged application dates and will require implementing acts.[31] Readers should verify the current rule before making operational or legal decisions.

Fourth, the comparative analysis does not claim that the United States, Minnesota, the European Union, and India are institutionally equivalent. They were selected because together they illustrate materially different approaches to licensure, reimbursement, and data integration. The policy recommendations identify functional principles that can be adapted, not a single model that should be copied verbatim.

Fifth, this review focuses on licensure, liability, reimbursement, and data governance. It does not comprehensively analyze controlled-substance prescribing, taxation, corporate practice of medicine, competition law, sanctions, export controls, medical-device regulation, artificial intelligence regulation, accessibility, or all consumer-protection laws. Those issues can materially affect particular cross-border business models and should be added to a transaction-specific compliance review.

9. Conclusion

Cross-border telemedicine has reached a stage at which legal infrastructure, not communications technology, is the principal constraint on scale. The systematic evidence and current legal frameworks converge on four interdependent requirements. A provider must have authority to practice across the relevant border; responsibility for clinical and technical failure must be allocated; payment must be available on predictable terms; and health data must be capable of moving securely and interoperably with the patient and care team.

The United States remains a patient-location, state-licensure system, but compacts and registration pathways provide increasingly important portability tools.[22-24] Minnesota shows how a state can reduce the administrative burden for qualifying out-of-state physicians while retaining jurisdiction and combine that approach with strong private-payer telehealth protections.[25,26,29] The European Union uses a provider-location rule for exclusively remote telemedicine under Directive 2011/24/EU, now clarified by DrSmile,[12,30] and is building a deeper data infrastructure through the EHDS.[31] India has a detailed domestic telemedicine framework and insurer guidance,[18,19,34] but international professional recognition remains a separate problem.

A durable cross-border framework should therefore aim for interoperability rather than regulatory absence. Portable professional authorization should preserve accountability; liability should follow defined functions and handoffs; reimbursement should be transparent and modality-neutral where clinically appropriate; and data portability should be treated as continuity-of-care infrastructure. The business case for cross-border digital health becomes stronger when these rules are designed together. More importantly, patients gain a clearer answer to four basic questions: who may treat me, who is responsible, who will pay, and where will my health information go.

Declarations

Ethics approval and consent to participate: Not applicable. This study is a systematic review and legal-policy analysis of published literature and public legal materials and did not involve human participants or identifiable private data.

Consent for publication: Not applicable.

Funding: No external funding was received for this work.

Competing interests: The author declares no competing interests.

Data availability: All materials analyzed in this review are publicly available through the open-access scholarly sources and official legal or regulatory repositories cited in the reference list. No new participant-level dataset was generated.

Author contributions: The author conceived the review, conducted the literature and legal-policy synthesis, interpreted the evidence, and prepared the manuscript.

Use of legal materials: This article is scholarly analysis and does not constitute legal advice. Statutory and regulatory requirements should be verified for the specific jurisdiction, profession, payer, and service before implementation.

References:

[1] Perrin Franck C, Azzabi S, Magdeleine J, Sauvé P, Muneene D, Labrique A. Policy analysis and expert consultation on cross-border telehealth services. Bull World Health Organ. 2026;104(6):427-434.

doi:10.2471/BLT.25.294599. PMCID: PMC13223688. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC13223688/

[2] Johnson D, Quinn S, Algase LF, Watkins C Jr; Medical Practice and Quality Committee of the American College of Physicians. Telemedicine policy and practice: a position paper from the American College of Physicians. Ann Intern Med. 2026;179(7):1030-1032. doi:10.7326/ANNALS-25-04194. Available from: https://pubmed.ncbi.nlm.nih.gov/42114091/

[3] Fields BG. Regulatory, legal, and ethical considerations of telemedicine. Sleep Med Clin. 2020;15(3):409-416. doi:10.1016/j.jsmc.2020.06.004. PMCID: PMC7340020. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC7340020/

[4] Jolin JR, Richman B, Mehrotra A, Shachar C. Reforming physician licensure in the United States to improve access to telehealth: state, regional, and federal initiatives. Milbank Q. 2024;102(4):833-852. doi:10.1111/1468-0009.12713. PMCID: PMC11654759. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC11654759/

[5] Rowland SP, Fitzgerald JE, Lungren M, Lee EH, Harned Z, McGregor AH. Digital health technology-specific risks for medical malpractice liability. NPJ Digit Med. 2022;5:157. doi:10.1038/s41746-022-00698-3. PMCID: PMC9581762. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9581762/

[6] Houser SH, Flite CA, Foster SL. Privacy and security risk factors related to telehealth services - a systematic review. Perspect Health Inf Manag. 2023;20(1):1f. PMCID: PMC9860467. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9860467/

[7] Bruthans J, Jiráková K. The current state and usage of European electronic cross-border health services (eHDSI). J Med Syst. 2023;47(1):21. doi:10.1007/s10916-023-01920-9. PMCID: PMC9918835. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9918835/

[8] Martins D, Lewerenz S, Carmo A, Martins H. Interoperability of telemonitoring data in digital health solutions: a scoping review. Front Digit Health. 2025;7:1502260. doi:10.3389/fdgth.2025.1502260. PMCID: PMC12052697. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC12052697/

[9] Carradinha M, Mendes VIS, Moura RP, Silva NP, Rocha L, Gonçalves J, et al. Telemedicine and the European Health Data Space: a new paradigm for healthcare in the EU. Front Digit Health. 2026;7:1713758. doi:10.3389/fdgth.2025.1713758. Available from: https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2025.1713758/full

[10] Van Delm K. EU in-home digital diagnostics - cross-border patient reimbursement under threat? In: Cohen IG, Kramer DB, Adler-Milstein J, Shachar C, editors. Digital Health Care outside of Traditional Clinical Settings: Ethical, Legal, and Regulatory Challenges and Opportunities. Cambridge: Cambridge University Press; 2024. p.196-210. doi:10.1017/9781009373234.019. Available from: https://www.cambridge.org/core/books/digital-health-care-outside-of-traditional-clinical-settings/eu-inhome-digital-diagnostics-crossborder-patient-reimbursement-under-threat/B3E6EF2B298005811635D2A3C2776FE4

[11] Campiglio C. EU cross-border telemedicine: a partial harmonisation of product and professional liability? European Papers. 2024;8(3):1539-1554. doi:10.15166/2499-8249/729. Available from: https://www.europeanpapers.eu/europeanforum/eu-cross-border-telemedicine-partial-harmonisation-product-professional-liability

[12] Court of Justice of the European Union. Judgment of the Court (Fourth Chamber) of 11 September 2025, UJ v Österreichische Zahnärztekammer, Case C-115/24, ECLI:EU:C:2025:694 [Internet]. Luxembourg: Court of Justice of the European Union; 2025 [cited 2026 Aug 29]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62024CJ0115

[13] Yeboah WK. The digital scalpel in cross-border telemedicine: slicing the medical act in DrSmile case. Eur J Risk Regul. 2026:1-7. doi:10.1017/err.2026.10109. Available from: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/digital-scalpel-in-crossborder-telemedicine-slicing-the-medical-act-in-drsmile-case/25F44E104870298429E0EAB022CC6832

[14] Elendu C, Amaechi DC, Elendu TC, Amaechi EC, Elendu ID, Omokore OA, et al. The legal and ethical considerations in cross-border telesurgical procedures. Ann Med Surg (Lond). 2025;87(6):3660-3672. doi:10.1097/MS9.0000000000003344. PMCID: PMC12140691. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC12140691/

[15] Ntafi C, Spyrou S, Bamidis P, Theodorou M. The legal aspect of interoperability of cross border electronic health services: a study of the European and national legal framework. Health Informatics J. 2022;28(3):14604582221128722. doi:10.1177/14604582221128722. Available from: https://journals.sagepub.com/doi/10.1177/14604582221128722

[16] Ftouni R, AlJardali B, Hamdanieh M, Ftouni L, Salem N. Challenges of telemedicine during the COVID-19 pandemic: a systematic review. BMC Med Inform Decis Mak. 2022;22(1):207. doi:10.1186/s12911-022-01952-0. Available from: https://link.springer.com/article/10.1186/s12911-022-01952-0

[17] Misheva K, Ampovska M. The legal aspects of telehealth. EU Comp Law Issues Chall Ser. 2022;6:393-409. doi:10.25234/eclic/22436. Available from: https://ojs.srce.hr/eclic/article/view/22436

[18] Dinakaran D, Manjunatha N, Kumar CN, Math SB. Telemedicine practice guidelines of India, 2020: implications and challenges. Indian J Psychiatry. 2021;63(1):97-101. doi:10.4103/psychiatry.IndianJPsychiatry_476_20. PMCID: PMC8106416. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC8106416/

[19] Venkatesh U, Aravind GP, Velmurugan AA. Telemedicine practice guidelines in India: global implications in the wake of the COVID-19 pandemic. World Med Health Policy. 2022;14(3):589-599. doi:10.1002/wmh3.497. PMCID: PMC9111269. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9111269/

[20] Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. 2021;372:n71. doi:10.1136/bmj.n71. Available from: https://www.bmj.com/content/372/bmj.n71

[21] Rethlefsen ML, Kirtley S, Waffenschmidt S, Ayala AP, Moher D, Page MJ, Koffel JB; PRISMA-S Group. PRISMA-S: an extension to the PRISMA statement for reporting literature searches in systematic reviews. Syst Rev. 2021;10(1):39. doi:10.1186/s13643-020-01542-z. Available from: https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/s13643-020-01542-z

[22] Health Resources and Services Administration. Licensing across state lines [Internet]. Rockville (MD): Telehealth.HHS.gov; 2025 [cited 2026 Aug 29]. Available from: https://telehealth.hhs.gov/licensure/licensing-across-state-lines

[23] Health Resources and Services Administration. Licensure compacts [Internet]. Rockville (MD): Telehealth.HHS.gov; updated 2025 Dec 10 [cited 2026 Aug 29]. Available from: https://telehealth.hhs.gov/licensure/licensure-compacts

[24] Interstate Medical Licensure Compact Commission. IMLCC snapshot statistics [Internet]. 2026 Aug 6 [data through 2026 Jul 31; cited 2026 Aug 29]. Available from: https://imlcc.com/

[25] Minnesota Legislature. Minnesota Statutes 2025, §147.032: Interstate practice of telehealth [Internet]. St Paul (MN): Minnesota Revisor of Statutes; 2025 [cited 2026 Aug 29]. Available from: https://www.revisor.mn.gov/statutes/cite/147.032

[26] Minnesota Legislature. Minnesota Statutes 2025, §147.033: Physician-patient relationship; telehealth [Internet]. St Paul (MN): Minnesota Revisor of Statutes; 2025 [cited 2026 Aug 29]. Available from: https://www.revisor.mn.gov/statutes/cite/147.033

[27] Centers for Medicare & Medicaid Services. List of telehealth services: Calendar Year 2026 [Internet]. Baltimore (MD): CMS; modified 2026 Mar 4 [cited 2026 Aug 29]. Available from: https://www.cms.gov/medicare/coverage/telehealth/list-services

[28] Centers for Medicare & Medicaid Services. Calendar Year 2026 Medicare Physician Fee Schedule final rule (CMS-1832-F) [Internet]. Baltimore (MD): CMS; 2025 [cited 2026 Aug 29]. Available from: https://www.cms.gov/newsroom/fact-sheets/calendar-year-cy-2026-medicare-physician-fee-schedule-final-rule-cms-1832-f

[29] Minnesota Legislature. Minnesota Statutes 2025, §62A.673: Coverage of services provided through telehealth (Minnesota Telehealth Act) [Internet]. St Paul (MN): Minnesota Revisor of Statutes; 2025 [cited 2026 Aug 29]. Available from: https://www.revisor.mn.gov/statutes/2025/cite/62A.673

[30] European Parliament and Council of the European Union. Directive 2011/24/EU of 9 March 2011 on the application of patients' rights in cross-border healthcare, consolidated text [Internet]. Brussels: EUR-Lex; 2011 [cited 2026 Aug 29]. Available from: https://eur-lex.europa.eu/eli/dir/2011/24/oj/eng

[31] European Parliament and Council of the European Union. Regulation (EU) 2025/327 of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [Internet]. Official Journal of the European Union; 2025 [cited 2026 Aug 29]. Available from: https://eur-lex.europa.eu/eli/reg/2025/327/oj/

[32] Health Resources and Services Administration. Privacy laws and policy guidance for telehealth [Internet]. Rockville (MD): Telehealth.HHS.gov [cited 2026 Aug 29]. Available from: https://telehealth.hhs.gov/providers/best-practice-guides/privacy-and-security-telehealth/privacy-laws-and-policy-guidance

[33] Ministry of Health and Family Welfare, Government of India. Telemedicine regulations [Internet]. New Delhi: Press Information Bureau; 2021 Jul 30 [cited 2026 Aug 29]. Available from: https://www.pib.gov.in/PressReleasePage.aspx?PRID=1740756

[34] Insurance Regulatory and Development Authority of India. Guidelines on Telemedicine. Ref No. IRDAI/HLT/REG/CIR/149/06/2020 [Internet]. Hyderabad: IRDAI; 2020 Jun 11 [cited 2026 Aug 29]. Available from: https://irdai.gov.in/document-detail?documentId=394669

[35] World Trade Organization. Services: health and social services [Internet]. Geneva: WTO [cited 2026 Aug 29]. Available from: https://www.wto.org/english/tratop_e/serv_e/health_social_e/health_social_e.htm