









Secure–Privacy–Ethical–Legal Governance Framework for Triage-Centric Telemedicine Workflows

S. Hemalatha¹, Govindharaju Karthi^{2*}, Mary Selvan³, A. Gnanasekar⁴, S. K. Satyanarayana⁵,
Bondalapu Chaitanya Krishna⁶

¹ Department of Computer Science and Business Systems, Panimalar Engineering College, Chennai 600123, India

² Department of Artificial Intelligence and Data Science, Saveetha Engineering College, Chennai 602105, India

³ Department of Artificial Intelligence and Data Science, R.M.K College of Engineering and Technology, Chennai 601206, India

⁴ Department of Computer Science and Engineering, R.M.D. Engineering College, Chennai 601206, India

⁵ Department of Electronic and Communication Engineering, Sreenidhi Institute of Science and Technology, Hyderabad 501301, India

⁶ Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522502, India

Corresponding Author Email: gkarthi@saveetha.ac.in

Copyright: ©2026 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijss.160120>

ABSTRACT

Received: 17 November 2025

Revised: 16 January 2026

Accepted: 24 January 2026

Available online: 31 January 2026

Keywords:

triage-centric telemedicine, telemedicine governance, workflow-level governance, Secure–Privacy–Ethical–Legal framework, stakeholder accountability, tele-prescription and dispensing compliance, regulatory enforcement

Telemedicine systems increasingly rely on digital triage workflows to manage patient access, consultation, prescribing, and medication dispensing. However, fragmented regulatory oversight and checklist-based compliance approaches have limited the enforceability and operational governance of these systems. This study presents a structured narrative review and proposes a Secure–Privacy–Ethical–Legal (SPEL) framework for triage-centric telemedicine workflows. The review analyzed 42 peer-reviewed research articles and 18 policy and regulatory documents published between 2019 and 2025, covering telemedicine security, privacy, ethics, and legal compliance. The literature synthesis revealed four dominant thematic categories: (i) secure identity verification and access control, (ii) privacy and data protection mechanisms, (iii) ethical responsibility and stakeholder accountability, and (iv) legal enforcement and penal provisions. Despite the breadth of existing guidance, three critical governance gaps were identified: the absence of workflow-level legal accountability across stakeholders, limited integration of ethical principles into technical system design, and inadequate enforcement mechanisms linking regulatory violations to specific operational stages. To address these gaps, the proposed SPEL framework reconceptualizes telemedicine triage as a continuous and auditable governance process, explicitly mapping security controls, ethical obligations, and legal liabilities to each stage of the workflow. The framework offers an enforcement-oriented model for telemedicine governance, providing practical guidance for regulators, system designers, and healthcare providers seeking to build legally compliant and ethically robust telemedicine ecosystems.

1. INTRODUCTION

When the development of Information and Communication Technologies (ICT) [1] spread widely into all the domains, one of the domains is telemedicine [2], also called healing at a distance. Initially, telemedicine was started in the 1970s with the support of the telephone, mail conversation [3]. Later, the World Health Organization (WHO) defined the term telemedicine/telemedicine by means of providing the treatment over a distance with the support of ICT equipment like communication devices, the Internet, Medical equipment, etc. [4]. WHO defines health innovation as improving systems, products, technologies, services, and policies, especially for vulnerable populations. Even the promotion and usage of telemedicine technology was accepted after the COVID-19 period [5]. When the electric and internet facilities are

incorporated into the telemedicine, it leads the device to be vulnerable to security and privacy issues. Ethical and legal issues play a major role in assuring the telemedicine usage between the patient and physician [6, 7].

Many countries, like the US, have initiated digital legal rules and regulations through policy initiatives [8]. The US defined the term US Centers for Medicare & Medicaid Services (CMS) for telemedicine, telemedicine-related terms [9]. Expansion of telemedicine in the US, including the payment parity, Insurance policies, and relaxed state licensure laws, etc. In March 2020, the U.S. HHS Office for Civil Rights (OCR) issued the Notification of Enforcement Discretion for telemedicine [10]. The Health Insurance Portability and Accountability Act (HIPAA) privacy and security enforcement was relaxed temporarily to support rapid telemedicine adoption [11]. Providers could use non-HIPAA compliant

communication tools (Zoom, Skype, FaceTime) in good faith. ‘Red Flags’ and ‘Red Tape’ telemedicine and pharmacy-level barriers to buprenorphine in the United States were carried out [12].

In the context of telemedicine, triage refers to the structured, pre-consultation decision-making process that determines patient identity verification, urgency classification, eligibility for remote consultation, physician assignment, diagnostic pathway selection, and authorization for downstream actions such as prescription and pharmacy dispensing. Unlike traditional in-person triage, telemedicine triage is digitally mediated and integrates technical controls, ethical safeguards, and legal compliance mechanisms. In this study, triage is treated not as a single step, but as a continuous, workflow-level governance process spanning patient onboarding, consultation, prescription, and medication delivery.

Later, Indonesia [13] and the United States [14] understood that to treat telemedicine as a component of human rights in healthcare. Added more values on regulation, informed consent, medical records, licensing, and prescriptions. Indonesia faces legal threats due to unclear regulations. Recommends adopting U.S. legal frameworks for stronger certainty. Southeast Asia (Indonesia, Malaysia, Singapore, Thailand, Vietnam) countries for supporting Guidelines Comparison. 24 guideline documents analysed across Southeast Asian countries [15]. The Domains covered are governance, ICT infra, data storage, privacy, ethics, and security. Singapore had the most comprehensive guidelines. This work recommends universal guidelines adaptable to the local context. Also reveals the key gaps on patient ID, data ownership, cyber laws, and record disposal.

The EU considers eHealth a top priority, introducing digital health care, policies, frameworks, etc. [16]. Legislative and regulatory journey of telemedicine in Organization for Economic Co-operation and Development (OECD) vs. non-OECD countries by adding stronger health system performance and Stakeholder collaboration essential for telemedicine planning and scalability [17]. India recommends stronger ethical frameworks within the guidelines [18]. But progress remains slow and inconsistent. Barriers: cultural resistance, poor infrastructure, lack of funding, and lack of IT skills. Recommends investment in public awareness, training, and national-level policies. Telemedicine in Brazil, The regulatory framework from the duration of 1990 to 2018, professional council regulations [19]. Used the advocacy coalition framework model. Finally, they conclude that despite many laws, Brazil still lacks a cohesive telemedicine regulatory framework.

Many countries keep promoting telemedicine growth by introducing several benefits and adaptations. Despite the rapid expansion of telemedicine platforms, existing studies and regulatory guidelines primarily address security, privacy, ethics, and legal compliance as isolated concerns or checklist-based requirements. There remains a lack of workflow-level governance models that explicitly operationalize telemedicine triage as a continuous decision-making process spanning patient authentication, consultation eligibility, tele-prescription, and pharmacy dispensing. Moreover, stakeholder accountability across physicians, pharmacies, platform providers, and regulators is weakly integrated into current technical and policy frameworks.

Accordingly, this study addresses the following research questions:

RQ1: How can telemedicine triage workflows be governed

through an integrated Secure–Privacy–Ethical–Legal (SPEL) framework that is enforceable across all stages of remote care delivery?

RQ2: How can stakeholder-specific accountability and legal liability be systematically mapped to tele-consultation, tele-prescription, and medication dispensing processes within digital health systems?

The key contributions of this study are as follows:

1. A structured narrative synthesis of recent telemedicine research and policy documents, identifying governance-level gaps in existing security, privacy, ethical, and legal guidelines.
2. A triage-centric SPEL framework that operationalizes governance as a continuous, auditable workflow rather than a static compliance checklist.
3. A stakeholder accountability mapping, explicitly linking physicians, pharmacies, platform providers, and regulators to enforceable legal and ethical responsibilities across tele-consultation and tele-prescription processes.
4. A penalty-aware governance perspective, demonstrating how regulatory violations can be traced to specific workflow stages to support enforcement and compliance.

Despite extensive national-level telemedicine regulations and ethical guidelines, there is a lack of an integrated, stakeholder-aware, legally enforceable, and privacy-preserving global SPEL framework that operationalizes legal and ethical compliance across patients, physicians, hospitals, pharmacies, and manufacturers. Existing studies focus on isolated legal issues, country-specific policies, or ethical principles, but do not provide a unified operational SPEL framework with enforcement mechanisms.

This article will address the above three issues by introducing the telemedicine strategy to avoid any kind of legal and ethical violation among the stakeholders, the pharmacy, the physician, and the patient. The article is organized such a way of discussing on systematic review methodology in Section 2, literature review analysis is done in Section 3, structure systemic finding is discussion in Section 4, the legal and ethical issues in telemedicine/telemedicine in followed by the proposed telemedicine SPEL framework in Section 5, scenario-based validation of the SPEL framework is discussion Section 6, ethical and legal issues cases in and around the world in Section 7, research directions for future legal and ethical issues in Section 8, finally end with the conclusion in Section 9.

2. METHODOLOGY

This study adopts a structured narrative review methodology combined with comparative legal and ethical analysis to examine security, privacy, ethical, and legal challenges in telemedicine. The methodology is designed to synthesize interdisciplinary evidence from healthcare, law, ethics, and digital health governance, with a focus on identifying regulatory gaps and informing the development of a unified telemedicine framework.

2.1 Review design

This study adopts a structured narrative review methodology, combining systematic search and screening

procedures with thematic synthesis. The approach was chosen to accommodate the interdisciplinary nature of telemedicine governance, spanning technical, ethical, and legal domains.

2.2 Data sources and search strategy

A systematic search of peer-reviewed literature and legal sources was conducted using major academic and legal databases, including Scopus, PubMed, IEEE Xplore, and Hein Online. These databases were selected to ensure comprehensive coverage of medical, technological, ethical, and legal perspectives relevant to telemedicine.

The search strategy employed combinations of keywords such as *telemedicine*, *digital health*, *privacy*, *security*, *ethics*, *legal framework*, *regulation*, *data protection*, and *healthcare law*. Boolean operators were used to refine and expand the search where appropriate.

2.3 Search strings

The following search string was used in Scopus:

(telemedicine OR Telemedicine OR "digital health") AND (triage OR workflow OR governance) AND (security OR privacy OR ethics OR legal OR compliance) AND (prescription OR pharmacy OR dispensing)

Similar keyword combinations were adapted for other databases based on their indexing syntax.

2.4 Screening and selection process

The initial database search yielded 154 records. After removing 54 duplicate entries, 100 titles and abstracts were screened for relevance. Studies were excluded if they were unrelated to telemedicine governance, lacked discussion of security, privacy, ethical, or legal aspects, or focused exclusively on clinical outcomes without workflow implications. Following abstract screening, 74 full-text articles were assessed for eligibility, resulting in 52 peer-reviewed studies included in the final synthesis as summaries in Table 1.

Table 1. Literature screening and selection summary

Stage	Number of Records
Records identified	154
Duplicates removed	54
Titles/abstracts screened	74
Full-text assessed	52
Studies included	42
Policy/legal documents	18

2.5 Selection of legal cases and policy documents

Legal cases and policy documents were selected using a purposive but transparent approach to minimize selection bias. Sources included official government portals, regulatory authority publications (e.g., health ministries, data protection authorities), and internationally recognized legal repositories. Only documents that (i) explicitly addressed telemedicine, digital health, e-prescription, or pharmacy regulation, and (ii) were publicly enforceable or officially issued were included. Landmark cases and policies were prioritized based on citation frequency, jurisdictional relevance, and applicability to telemedicine workflows, resulting in 18 policy and legal documents included in the review.

2.6 Data extraction and synthesis

Extracted data included study focus, governance dimension addressed, stakeholder scope, and identified limitations. A thematic synthesis approach was applied to group studies into governance domains and identify cross-cutting gaps that informed the development of the SPEL framework.

3. LITERATURE REVIEW: A THEMATIC SYNTHESIS

This section presents a comprehensive literature survey organized across five key dimensions of telemedicine security, privacy, ethics, legal considerations, and existing frameworks. The review begins by examining the rapid growth of telemedicine during the COVID-19 period, followed by a detailed discussion on privacy and security issues, ethical guidelines, various country-specific telemedicine initiatives, and prevailing legal challenges. The survey incorporates the most recent research articles published between 2020 and 2025.

3.1 Privacy and security threats in telemedicine workflows

A review [20] on protection of patient data in digital oral and general health care examined digital health and tele dentistry expanded during COVID-19. The article Metrics/Focus Areas: 24 articles reviewed (scoping review), Data security policies are most frequently studied and find gaps in: informed consent standards, clinical liability definitions, confidentiality measures. The authors' major concerns are data security, privacy, ethical risks, and inconsistent standards. Need for unified regulations and app control systems. Rise of "patient 4.0" increasing medico-legal pressures. A systematic review [21] examined privacy and security risk factors related to telemedicine services. They identified privacy and security risk factors during telemedicine expansion (COVID-19 context). Risks classified into environmental, technology, and operational factors. Metrics/Findings from 18 empirical studies: Environmental: lack of private space, difficulty sharing sensitive info. Technology: weak data security, poor internet access. Operational: reimbursement issues, training gaps, tech accessibility. Finally, authors develop best practices for privacy in telemedicine, improve training for providers and patients, and expand policies ensuring technology accessibility and secure environments.

Despite extensive technical countermeasures, these studies largely treat security and privacy as system-level concerns, with limited attention to workflow-specific accountability or legal enforceability.

3.2 Consent management and clinical documentation

The previous study [22] carried out the research review on telemedicine and ethics: opportunities in India, specifically focusing on ethical issues. Their review works reveal the following point to improve in India: telemedicine guidelines (2020) improve legal clarity. Ethical issues still unresolved: consent, documentation, patient identity verification, and autonomy. Recommends stronger ethical frameworks within the guidelines. The comparison of telemedicine-related ethics and guidelines and a checklist for ethical decision making in behavioral analysis practice was carried out in the USA to

support ethics in ABA telemedicine [23]. They compared ethics codes from psychology, paediatrics, and social work with ABA. Identified unique ethical concerns for ABA telemedicine that have not been addressed previously. Created a telemedicine readiness checklist (legal, professional, and ethical requirements).

3.3 Licensure, liability, and professional accountability

Discussing the legal aspects of the use of AI in telemedicine was carried out in the study [24], focusing on Global AI Law, Privacy, and Continuous Learning Systems. They point out the following points that AI plus telemedicine increases privacy and consent risks. Continuous learning systems create additional liability and ethical risks. Vulnerable groups (children, the elderly, and the severely ill) face issues with free consent. The study proposes safeguards and legal recommendations to minimize risks. Researchers have conducted a review [25] on applications of medico-legal challenges of telemedicine in ophthalmology. Finally, this article reveals the following points: treat telemedicine as a component of human rights in healthcare. Major differences: regulation, informed consent, medical records, licensing, prescriptions. Indonesia faces legal threats due to unclear regulations. Recommends adopting U.S. legal frameworks for stronger certainty.

Application fields, professional liability and focus on care services during the COVID-19 in Italy for telemedicine medical legal aspects of was discussed in the study [26]. Legal issues include accreditation, confidentiality, consent, and developing parallel regulatory infrastructures, which strengthen legal clarity on liability and data protection. Finally, Italy's telemedicine classifications: Specialized Telemedicine, Tele-healthcare, Tele-assistance for service center, facility, healthcare worker. Researchers [27] discussed the following points in telemedicine expands access but introduces legal/regulatory challenges, Physician licensure becomes complex across states, Interstate Medical Licensure Compact provides simplified multistate licensure, Physician-patient relationship, informed consent, and standard of care gain added layers in telemedicine also projected providers must follow both state laws (provider location plus patient location) and federal laws (Ryan Haight Act, HIPAA, Stark Law, Anti-Kickback Statute). But the authors find the following points were difficult to address: Compliance burden across states (no direct metrics but regulatory complexity), Legal risk assessment (qualitative). Multistate licensure efficiency improved by the Compact (process metric).

The legal, regulatory, and ethical issues for cell phone stewardship framework were examined in the study [28]. They evaluated WhatsApp usage data from 590 articles. Categorized issues into legal, regulatory, and ethical. Points highlighted are Rapid use of WhatsApp in clinical care requires oversight, identified legal, ethical, and regulatory challenges, and developed the Cell Phone Stewardship Framework for Healthcare Professionals (CSF-HCP). The author's recommendation was to promote "cell phone stewardship" and Formal adoption of CSF-HCP across healthcare organizations.

The ethical, legal, and social challenges in the development and implementation of disaster telemedicine were examined in the study [29]. She evaluates the crisis standards of care and quality assurance, and preparedness indicators. And insist on the following point, telemedicine is critical during disaster

response, raises ethical, social, and legal challenges, and needs disaster-specific telemedicine standards. The author recommends developing ethical frameworks for disaster telemedicine and creating public-private partnerships for scalable systems.

3.4 Cross-border telemedicine governance

Telemedicine in Middle Eastern countries, including its progress, barriers, and policy recommendations, was discussed in the study [6] during COVID. They find the Adoption Barriers, Policy, but this work also pointed out the following discussions: Progress remains slow and inconsistent. Barriers: cultural resistance, poor infrastructure, lack of funding, and lack of IT skills. Recommends investment in public awareness, training, and national-level policies. 'Red Flags' and 'Red Tape' telemedicine and pharmacy-level barriers to buprenorphine in the United States was carried out in the study [12]. This work was carried out with participant observations and semi-structured interviews: Patients (n = 19), prescribers (n = 24), pharmacists (n = 10) in PA and CA (2020–2021). The points highlighted in this article are COVID-19 enabled telemedicine exemptions for buprenorphine prescribing, but pharmacy barriers remained. Study examines telemedicine implementation for Opioid Use Disorder (OUD) treatment. Due to this work, telemedicine increased access, but pharmacies still imposed "red flags" and "red tape" such as geographic restrictions, cancellations, and refusals. Barriers led some patients to relapse into injection drug use. But limits on telemedicine alone cannot eliminate access barriers. Pharmacy-level practices influenced by DEA fears continue to restrict treatment, producing uneven policy impacts.

A review on telemedicine guidelines in Southeast Asia (Indonesia, Malaysia, Singapore, Thailand, and Vietnam) was conducted in the study [30] to support guideline comparison. 24 guideline documents analyzed across SE Asian countries. The Domains covered are governance, ICT infra, data storage, privacy, ethics, and security. Singapore had the most comprehensive guidelines. This work recommends universal guidelines adaptable to the local context. Also reveals the key gaps on patient ID, data ownership, cyber laws, and record disposal. A set of researchers [11] have shown the importance of the HIPAA and Accelerated telemedicine adoption during COVID-19 in the USA, which is titled HIPAA telemedicine adoption. This article highlighted that COVID-19 forced rapid telemedicine adoption; HIPAA enforcement was temporarily relaxed. Non-EMR apps are used widely but lack the required Audit Controls. Many apps are encrypted but still not HIPAA-compliant. Suggests revising HIPAA audit rules to improve care while protecting privacy. Highlights legal/ethical issues: liability, cybersecurity, scope of practice.

How telemedicine is becoming the new normal in the European Union due to rapid digital transformation was discussed in the study [31]. The EU considers eHealth a top priority (Digital Health and Care 2018; EC 2019–2024 priorities). COVID-19 accelerated telemedicine integration into traditional systems. Major challenge: lack of telemedicine-specific legislation, policies, and governance frameworks in the EU and especially in North Macedonia.

The following points were mentioned in the study [32]: WHO defines health innovation as improving systems, products, technologies, services, and policies, especially for vulnerable populations. The study explored the legislative and

regulatory journey of telemedicine in OECD vs. non-OECD countries. The sources reviewed: government documents, medical board reports, media, and peer-reviewed literature. Legislation/regulation essential for governance, accountability, safety, and security. No uniform global telemedicine legislation; countries use different strategies (including precautionary approaches). Telemedicine implementation styles vary widely. But need to move beyond regulation for stronger health system performance, and Stakeholder collaboration is essential for telemedicine planning and scalability.

3.5 Tele-prescription and pharmacy dispensing controls

The implementation of a law enforcement-led pre-arrest diversion-to-treatment program for adults with substance use disorders was discussed in the study [33]. The study describes implementation and outcomes of a pre-arrest diversion program (MARI). This article focuses on Formative plus process evaluation, descriptive statistics, thematic qualitative analysis, and the dataset from Sept 2017–Aug 2020, and elaborates on the surveys from police, participants, and treatment staff. There were 263 participants who engaged and completed the program. The previous study [34] highlighted the COVID-19 triggered rapid and unprecedented expansion of telemedicine in the US. Regulatory changes during PHE include: payment parity, relaxed HIPAA enforcement, and relaxed state licensure laws. The Payment parity addressed low reimbursement barriers; telemedicine visits increased from ~ 10% to > 90% in many clinics. Also, the privacy rules were relaxed, allowing non-HIPAA platforms (FaceTime, Zoom). States relaxed licensure rules; clinicians could treat across state borders.

It was emphasized in the study [35] that the telemedicine providers must comply with institutional, state, and federal regulations, and it is mandatory to obtain multistate licensing

when providing care across state lines, as well as credentialing and privileging required at external facilities. Internet-based prescribing has legal restrictions and is allowed only under limited conditions. Also, the Malpractice insurance coverage for telemedicine varies by insurer, especially for interstate telemedicine. Telemedicine programs must uphold strict PHI protection. Ethical principles (autonomy, beneficence, non-maleficence, justice) apply equally to telemedicine and in-person care. Telemedicine has more similarities than differences with traditional practice. Need to streamline regulatory processes to unlock telemedicine’s full potential. But this work has a high administrative burden to comply with all federal/state rules.

The following points were pointed out in the study [36]. COVID-19 increased the need for telemedicine. Telemedicine reduces exposure, frees hospital resources, and improves access for rural areas. Regulators removed barriers rapidly. Telemedicine benefits will remain after COVID-19. Key focus areas for improvement: reimbursement, privacy and cybersecurity, liability, licensure, tech access, and AI integration. Need for monitoring how companies use transmitted personal health data. But this article finds some limitations on the legal services, telemedicine utilization rates during COVID, Regulatory compliance (HHS, FDA, state updates), Patient access indicators (rural vs. urban), and data security/cybersecurity compliance. De-metrics (Gaps), Inconsistent reimbursement models. Unclear malpractice and liability frameworks, technology access inequality, and limited AI regulations.

Three decades of telemedicine in Brazil, including the regulatory framework from 1990 to 2018, were discussed in the study [37]. Mapping and content analysis of 79 federal legislations with 31 professional council regulations. Used the advocacy coalition framework model. Finally, they conclude that despite many laws, Brazil still lacks a cohesive telemedicine regulatory framework.

Table 2. Thematic mapping of telemedicine governance literature

Theme	Representative Studies	Primary Focus	Key Limitation / Gap
Privacy and security	[20-22]	Encryption, access control	No workflow-level legal mapping
Consent and documentation	[22, 23]	Digital consent models	Weak downstream enforcement
Licensure and liability	[24-29]	Physician accountability	Jurisdiction-specific focus
Cross-border governance	[30-35]	Regulatory compliance	Policy-level only
Tele-prescription and dispensing	[36, 37]	E-prescription safety	Limited pharmacy accountability

The thematic synthesis highlights in Table 2 that while telemedicine governance has been widely studied, existing approaches remain fragmented across technical, ethical, and legal dimensions. Security and privacy solutions are predominantly system-centric, consent mechanisms lack downstream enforceability, liability models are jurisdiction-bound, and pharmacy-level controls are insufficiently governed. Crucially, no existing SPEL framework integrates these dimensions into a unified, triage-centric workflow with explicit stakeholder accountability and enforceable legal mapping. This gap motivates the development of the proposed SPEL framework.

4. STRUCTURED “SYNTHESIS OF FINDINGS”

This review synthesizes findings from technical studies, legal analyses, and policy documents across multiple jurisdictions, including the European Union, the United States,

and India. Rather than reiterating individual study outcomes, this section consolidates cross-cutting patterns and governance gaps that consistently emerge across regulatory contexts. These synthesized findings directly inform the design choices embedded in the proposed SPEL framework.

4.1 Cross-jurisdictional governance patterns

Thematic synthesis reveals the following recurring patterns:

- Security and privacy controls are largely system-centric, focusing on encryption and authentication, with limited linkage to triage-centric telemedicine workflow-level accountability or legal enforcement.
- Consent mechanisms are inconsistently operationalized, often treated as one-time acknowledgements rather than enforceable, purpose-bound controls across downstream processes.
- Professional licensure and liability frameworks vary significantly across jurisdictions, creating ambiguity in

cross-border telemedicine practice and enforcement.

- Tele-prescription and pharmacy dispensing controls are uneven, with pharmacy-level accountability often weaker than physician-level regulation.
- Secondary data use and retention practices lack harmonization, increasing the risk of misuse beyond the original care context.

These patterns are observed consistently despite jurisdictional differences in legal terminology and enforcement mechanisms.

4.2 Key governance gaps identified

Based on the synthesis, the following structural gaps are identified:

- Gap 1: Absence of triage-centric telemedicine workflow-level governance.

Most regulations and guidelines do not map compliance requirements to concrete telemedicine triage-centric telemedicine workflow stages (triage, consultation, prescription, dispensing).

- Gap 2: Fragmented stakeholder accountability. Responsibilities of patients, physicians, pharmacies, platforms, and regulators are addressed in isolation, rather than as an integrated governance chain.

- Gap 3: Weak enforcement traceability. Existing frameworks rarely support post-hoc auditability or legal traceability when violations occur.

- Gap 4: Inadequate controls for insider misuse and secondary data sharing.

Insider threats and non-clinical data use are insufficiently governed by current technical or policy mechanisms.

4.3 Research gaps to Secure–Privacy–Ethical–Legal design mapping matrix

Table 3 collectively, these synthesized findings demonstrate the need for an integrated governance SPEL framework that operationalizes security, privacy, ethical responsibility, and legal compliance as interdependent triage-centric telemedicine workflow decisions, motivating the design of the proposed SPEL framework.

Table 3. Mapping of synthesized governance gaps to Secure–Privacy–Ethical–Legal (SPEL) design choices

Synthesized Gap	Cross-Jurisdiction Evidence	SPEL Design Choice	SPEL Dimension
Gap 1: Triage-centric telemedicine workflow-level governance missing	EU, US, and India guidelines treat controls as static	Triage-centric, stepwise triage-centric telemedicine workflow model	S, E, L
Gap 2: Fragmented accountability	Physician-focused liability dominates	Stakeholder role mapping with enforceable duties	E, L
Gap 3: Lack of traceability	Limited audit requirements	Mandatory audit logging and legal attribution	L
Gap 4: Insider and secondary misuse	Weak internal controls	Role-based access control (RBAC), consent-bound access, and retention policies	S, P
Gap 5: Pharmacy oversight gaps	Variable e-prescription enforcement	Pharmacy verification and dispensing controls	S, L

5. SECURE–PRIVACY–ETHICAL–LEGAL TELEMEDICINE FRAMEWORK

From the literature survey, many authors were discussing the security, privacy, legal, and ethical challenges in telemedicine handled by different countries. Even though the globalized SPEL framework, which supports all telemedicine challenges, was not invented by any inventor. The proposed SPEL framework operationalizes telemedicine triage as a legally enforceable and ethically governed triage-centric telemedicine workflow, where access control, consultation eligibility, prescription authorization, and pharmacy dispensing are all treated as sequential triage decisions. This section proposed a SPEL Framework, which will monitor or handle the telemedicine routing work, also supporting the patient, physician, pharmacy, and hospitals from violating ethical and legal issues. Figure 1 depicts the proposed SPEL framework, which has nine major process components, and each component is related to or connected to other components to achieve the globalized proposed SPEL framework. Each process component is named as Secure, Privacy, Ethical, Legal, Stakeholder, Pharmacy, Hospital, Patient, and Physician. The operational principle involved in each process is connected to other processes. Simple one-time password generation is majorly involved in the SPEL framework operation to ensure ethical and legal avoidance.

5.1 Threat model for triage-centric telemedicine workflows

The proposed SPEL framework assumes an adversarial environment encompassing both external and internal threat actors. The primary threat categories considered include:

- External attacks, such as unauthorized access, credential theft, and interception of telemedicine communications;
- Insider misuse, including unauthorized data access by clinicians, platform administrators, or pharmacy staff;
- Workflow abuse, such as prescription manipulation, illegal dispensing, or bypassing consent requirements; and
- Secondary data misuse, involving unauthorized data sharing for non-clinical or commercial purposes.

These threats are analyzed across the full telemedicine triage workflow, spanning patient onboarding, consultation, tele-prescription, pharmacy dispensing, and data retention.

Table 4 discusses the minimum required controls and its purpose.

5.2 Role and limitations of one-time password in the Secure–Privacy–Ethical–Legal framework

Within the SPEL framework, one-time passwords (OTPs) are employed as a first-layer authentication mechanism to verify user presence and session legitimacy during critical workflow transitions, such as login, prescription authorization,

and pharmacy verification. OTPs are effective against credential reuse, replay attacks, and certain forms of external intrusion. However, OTPs alone are insufficient to mitigate insider misuse, privilege abuse, or unauthorized secondary data sharing. For these risks, the SPEL framework explicitly

relies on role-based access control (RBAC), action-level audit logging, consent-bound data access, and enforceable retention and deletion policies. OTPs, therefore, function as a gatekeeping mechanism rather than a comprehensive security solution.

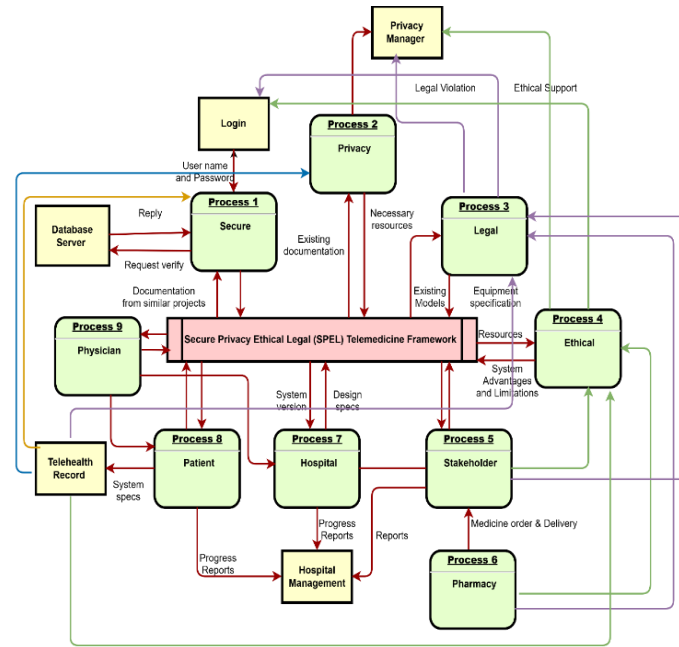


Figure 1. Secure-Privacy-Ethical-Legal (SPEL) telemedicine framework

Table 4. Minimum technical and organizational controls in the Secure-Privacy-Ethical-Legal (SPEL) framework

Control Category	Minimum Requirement	Purpose
Identity and authentication	One-time password (OTP) + primary credential	Prevent unauthorized access
Authorization	Role-based access control (RBAC)	Restrict actions by role
Consent management	Explicit digital consent capture	Ensure patient autonomy
Audit logging	Immutable access and action logs	Enable accountability
Prescription control	Physician-bound digital signatures	Prevent prescription forgery
Pharmacy verification	Licensed pharmacy validation	Prevent illegal dispensing
Data retention	Policy-based retention schedules	Limit over-retention
Data deletion	Enforced deletion/anonymization	Prevent misuse
Organizational policy	Defined stakeholder responsibility	Legal accountability

5.3 Mitigating insider misuse and secondary data sharing

Insider threats and secondary data misuse represent governance risks that cannot be adequately addressed through authentication alone. In the SPEL framework, insider misuse is mitigated through least-privilege role assignment, continuous audit logging of data access and modifications, and post-hoc legal traceability enabled by immutable records. Secondary data sharing is controlled through purpose-limited consent capture, role-specific data views, and policy-enforced retention and deletion mechanisms. These controls collectively ensure that data access is both technically constrained and legally attributable.

5.4 Legal and ethical framework

The legal and ethical framework is a library for handling ethical issues. For example, users entered the wrong OTP many times, trying to access the private data, stakeholder rules violation, pharmacy fraud, hospital-related issues, patient and Physician relationship, payment, etc. Tables 5-7 state the punishment in telemedicine legal issues globally in all kinds

of processes. Steps involving the legal and ethical framework process are given below.

Steps: Legal and Ethical Framework

1. Violation Monitoring

System continuously monitors for violations:

- Repeated wrong OTP attempts
- Accessing private data without consent
- Stakeholder rule violations
- Pharmacy fraud
- Physician-patient disputes
- Wrong billing or payment issues

2. Action Trigger

If a violation is detected:

- Log event
- Notify concerned authorities
- Trigger legal procedure or warning based on severity.

The following Tables 5-7 summarize penalties by legal regime. Each jurisdiction has distinct enforcement mechanisms and penalty structures; they are not interchangeable.

Table 5. Penalties for data protection violations in India

Legal Regime	Violation	Penalty	Source
DPDP Act, 2023	Breach of security safeguards	Up to ₹250 crore	Sethi et al. [38]
DPDP Act, 2023	Failure to notify of a breach	Up to ₹200 crore	
DPDP Act, 2023	Breach of duties (minor)	₹10,000	

Table 6. Penalties under General Data Protection Regulation (GDPR) (EU)

Legal Regime	Nature of Violation	Maximum Administrative Fine	Source
GDPR	Severe violation	Up to 4% global turnover or €20 million	Sood et al. [39]
GDPR	Lesser violation	Up to 2% global turnover	

Table 7. Penalties under Health Insurance Portability and Accountability Act (HIPAA) (US)

Legal Regime	Violation Category	Penalty Range	Source
HIPAA	Tier 1: No knowledge	\$100–\$50,000 per violation (annual cap varies)	https://www.bajajfinserv.in
HIPAA	Tier 4: Willful neglect not corrected	\$50,000 per violation (cap ~\$1.5M annually)	
HIPAA	Criminal offences	Up to \$250,000 and imprisonment	

6. SCENARIO-BASED VALIDATION OF THE SECURE-PRIVACY-ETHICAL-LEGAL FRAMEWORK

These scenarios given in Tables 8 and 9 demonstrate how the proposed SPEL framework operationalizes telemedicine

triage as a sequence of enforceable governance decisions rather than isolated technical steps. Each workflow action is explicitly linked to security controls, privacy safeguards, ethical obligations, and legal compliance requirements, enabling traceability, accountability, and regulatory oversight across the telemedicine lifecycle.

Table 8. Secure-Privacy-Ethical-Legal (SPEL) mapped triage workflow

Step	Input	Actor	Decision / Action	Output	SPEL Component	Compliance Requirement
1	Patient request	Patient	Identity verification via credentials + one-time password (OTP)	Authenticated session	S	Secure authentication
2	Health complaint	Platform	Triage classification (urgency, eligibility)	Tele-consult eligible	E, L	Fair access, duty of care
3	Consent form	Patient	Digital consent capture	Consent record	P, E	Informed consent
4	Case data	Physician	Role-verified consultation	Diagnosis	S, E	Licensed practice
5	Prescription	Physician	Digitally signed e-prescription	Valid prescription	L	Medical liability
6	Prescription + OTP	Pharmacy	License verification + OTP	Drug dispensed	S, L	Pharmacy regulation
7	Session data	Platform	Audit logging	Immutable logs	L	Legal traceability
8	Medical data	System	Retention / deletion enforcement	Policy-compliant storage	P, L	Data protection law

Table 9. Secure-Privacy-Ethical-Legal (SPEL) enforcement against insider threats

Step	Input	Actor	Decision / Action	Output	SPEL Component	Requirement
1	Patient record	Pharmacy staff	Access attempt beyond role	Access denied	S	RBAC enforcement
2	Access request	System	Audit logging triggered	Log entry	L	Accountability
3	Repeated access	System	Alert raised	Admin notified	S, L	Incident reporting
4	Log review	Compliance officer	Misuse identified	Policy violation	E, L	Ethical breach
5	Data policy	System	Retention and restriction enforced	Data protected	P	Data minimization

7. ETHICAL AND LEGAL ISSUES CASES IN AND AROUND THE WORLD

Hageseth v. Superior Court in the USA, a psychiatrist licensed in Colorado prescribed fluoxetine via the Internet to a patient in California, without a face-to-face evaluation. The

patient later died by suicide. The court convicted the doctor of practicing medicine without a license, which underscores jurisdiction/licensure issues in remote prescribing and the risk of serious harm if remote evaluation is inadequate. Telemedicine malpractice and standard-of-care lawsuits [40] in the USA, Cases where remote consultations (e.g., for ear

pain, dermatology via photo uploads) led to misdiagnosis or missed diagnosis (e.g., melanoma), claims argued a lack of in-person exam or informed consent. As highlighted in malpractice law literature, reinforces that telemedicine must meet the same standard of care as in-person care; tele-providers are liable for negligence even if consultation was virtual. Cross-state / interstate telemedicine liability and regulatory conflicts [36] in the USA, in federated systems, licensing boards may not have enforcement over out-of-state providers; jurisdictional complexity hampers accountability for cross-state telemedicine. Regulatory ambiguity, cross-state telemedicine may evade standard oversight, complicating malpractice claims/liability/professional discipline. Regulatory-board restrictions: prior in-person requirement for electronic consultation [41] in the USA. Historically, in some states (e.g., Idaho), electronic-only consultations/prescriptions were disallowed; in other states, providers challenged such rules (e.g., Teladoc Health vs. state boards). Demonstrates how regulation (or its absence) can limit or enable telemedicine; restrictive rules can hinder access, especially affecting rural/underserved areas, but relaxations may bring regulatory risk or compromise quality.

Early medico-legal analysis: Telemedicine in India: an ethical and medico-legal perspective in India [42], highlighted the lack of a clear-cut legal/regulatory framework for telemedicine; identified medico-legal issues: doctor-patient relationship, consent, confidentiality, medical negligence, liability, licensing, and jurisdiction. Shows that even where telemedicine is used, a lack of formal regulation can lead to legal/ethical ambiguity, risk for both providers and patients in virtual care delivery. Recent legal-ethical review: Legal Challenges and Considerations in Implementing Telemedicine Services [43] in India, Analysis of existing guidelines (e.g. Telemedicine Practice Guidelines, Medical Council and IT law), found gaps related to licensing, liability, credentialing, data privacy; also raised ethical issues: informed consent, equitable access, patient privacy, maintenance of care quality in virtual consultations. Underlines continuing legal and ethical vulnerabilities in telemedicine practice in India, especially regarding privacy, consent, liability, and equitable access in rural/underserved contexts. Ethical and legal aspects of telepsychiatry [44] in India, as telepsychiatry grows, need for explicit definitions: what constitutes a valid virtual consultation, prescription modes, documentation, and eligible platforms; current frameworks are inadequate for some aspects. Emphasizes that specialty tele-services (e.g., psychiatry) via telemedicine require clearer legal/ethical standards to ensure safe, responsible remote care.

In a systematic review of telemedicine during COVID-19 reported in the study [45] that rural populations had difficulty accessing telemedicine due to a lack of infrastructure, limited digital literacy, and a lack of regulation, concerns around data confidentiality/security, challenges in lab tests, prescriptions, and diagnostics. Demonstrates that in LMICs, rural/infrastructure limitations make telemedicine risky: quality of care, confidentiality, and equitable access threaten to worsen health disparities. Same review remote monitoring and telemedicine for heart disease / general care [46] in ITALY, Problems: low patient adherence/cooperation, poorly structured data management, device issues, data privacy, lack of uniform reimbursement, informed consent, and training gaps; telemedicine not suitable for emergencies; diagnostics limitations. Highlights that even in higher-income countries, telemedicine faces cultural, systemic, regulatory, and

technological hurdles; quality, privacy, reimbursement, and standardization remain issues.

Rural hospitals – computer-mediated synchronous communication study: Improving Computer-Mediated Synchronous Communication of Doctors in Rural Communities through Cloud Computing [47] in South Africa, found that rural hospitals attempted tele-consultation / remote advice via computer-mediated tools, but frequent internet slowness, power outages, lack of e-health software, and poor connectivity hindered use. Demonstrates infrastructural and reliability barriers in rural/remote settings, telemedicine adoption is heavily constrained by connectivity/power, limiting scalability and equity. Brilliant AI Doctor in Rural China: Tensions and Challenges in AI-Powered CDSS Deployment [48] in China (rural clinics), Implementation of AI-powered clinical decision support systems (CDSS) in rural clinics, but clinicians reported misalignment with local workflows, technical limitations, usability barriers, limited transparency and trust; concerns about reliability. Raises ethical and practical concerns about deploying AI/Telemedicine jointly in rural/low-resource contexts: trust, usability, data quality, transparency, i.e., tele-solutions cannot be “one-size-fits-all.” Ethical and legal challenges of telemedicine in the era of the COVID-19 pandemic [49] in Multiple Countries (Global / Cross-jurisdiction), Found common issues across countries: informed consent, patient privacy/confidentiality, data protection/security, malpractice / professional liability, equity of access, quality of care, doctor-patient relationship, telemedicine often treated as supplement to in-person care rather than replacement. Indicates that regardless of country, telemedicine without robust regulation and safeguards carries risks [50]; privacy, equity, liability, and quality of care must be well-managed.

8. RESEARCH DIRECTIONS FOR FUTURE LEGAL AND ETHICAL ISSUES

Future research direction of legal and ethical issues focuses on the research areas of Cross-Border Telemedicine, Data Privacy and Security [51].

AI and Decision-Making, Informed Consent, Standard of Care [52], Equity and Access, Insurance and Reimbursement, IoT and Remote Mobile Monitoring system [53-56].

Telepsychiatry and Policy and Regulatory Foresight. By focusing on answering the following Questions.

1. How to harmonize international telemedicine laws?
2. How to mitigate data breaches and comply with privacy laws?
3. Liability and bias in AI-assisted telemedicine
4. How to ensure patient understanding remotely?
5. What constitutes acceptable telemedicine practice?
6. Does telemedicine reduce or worsen disparities?
7. How to ensure fair coverage?
8. Who is responsible for device errors?
9. How to ethically manage crises remotely?

9. CONCLUSIONS

This study presented a structured synthesis of telemedicine governance literature and proposed the SPEL framework as a triage-centric, workflow-oriented approach to integrating security, privacy, ethical responsibility, and legal compliance

in digital health systems. Rather than asserting universal enforceability or risk elimination, the framework is intended to support jurisdiction-aware governance by making compliance obligations explicit, auditable, and traceable across telemedicine workflows. The review identified recurring governance gaps across jurisdictions, including fragmented stakeholder accountability, limited workflow-level enforcement, and insufficient controls for teleprescription and pharmacy dispensing. By mapping these gaps to concrete SPEL design choices, the framework provides a conceptual foundation for translating regulatory intent into operational system requirements, without presuming uniform legal harmonization or automatic prevention of misuse. From a practical perspective, SPEL is best understood as an enabling governance model rather than a self-enforcing solution. Its effectiveness depends on institutional adoption, regulatory oversight, and organizational compliance practices. Telemedicine platforms, healthcare institutions, and regulators play complementary roles in operationalizing SPEL through role-based controls, audit mechanisms, and jurisdiction-specific enforcement processes.

Future work should focus on three concrete directions. First, policy harmonization pathways can be explored by aligning SPEL workflow stages with emerging international digital health standards, enabling interoperability without conflating legal regimes. Second, implementation-ready checklists derived from SPEL can be developed to guide platform designers and healthcare providers in translating governance principles into deployable controls. Third, empirical studies and pilot deployments are needed to evaluate how SPEL-informed systems perform under real-world regulatory audits and cross-border operational constraints. By situating governance within executable telemedicine workflows, the SPEL framework contributes a structured, review-informed perspective that can inform both policy discourse and system design, while remaining appropriately scoped to the conceptual nature of the present work.

REFERENCES

- [1] Saba, C.S., Ngepah, N., Odhiambo, N.M. (2023). Information and Communication Technology (ICT), growth and development in developing regions: Evidence from a comparative analysis and a new approach. *Journal of the Knowledge Economy*, 15(3): 14700-14748. <https://doi.org/10.1007/s13132-023-01571-8>
- [2] Nordin, S., Sturge, J., Ayoub, M., Jones, A., McKee, K., Dahlberg, L., Meijering, L., Elf, M. (2021). The role of Information and Communication Technology (ICT) for older adults' decision-making related to health, and health and social care services in daily life—A scoping review. *International Journal of Environmental Research and Public Health*, 19(1): 151. <https://doi.org/10.3390/ijerph19010151>
- [3] Gogia, S. (2020). Rationale, history, and basics of telehealth. In *Fundamentals of Telemedicine and Telehealth*, pp. 11-34. <https://doi.org/10.1016/B978-0-12-814309-4.00002-1>
- [4] Shende, V., Wagh, V. (2024). Role of telemedicine and telehealth in public healthcare sector: A narrative review. *Cureus*, 16(9): e69102. <https://doi.org/10.7759/cureus.69102>
- [5] Nichelatti, M. (2025). A preamble: What is and what telemedicine is for. In *Mathematical Tools for Telemedicine*, pp. 3-9. https://doi.org/10.1007/978-3-031-81709-0_1
- [6] Solimini, R., Busardò, F.P., Gibelli, F., Sirignano, A., Ricci, G. (2021). Ethical and legal challenges of telemedicine in the era of the COVID-19 pandemic. *Medicina*, 57(12): 1314. <https://doi.org/10.3390/medicina57121314>
- [7] Afzal, J. (2024). Best practice of digital laws and digital justice. In *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, pp. 95-120. https://doi.org/10.1007/978-981-97-7106-6_5
- [8] Davtyan, T. (2025). The U.S. approach to AI regulation: Federal laws, policies, and strategies explained. *Journal of Law, Technology & the Internet*, 16(2). <https://scholarlycommons.law.case.edu/jolti/vol16/iss2/2>.
- [9] Verma, S. (2020). Early impact of CMS expansion of Medicare telehealth during COVID-19. *Health Affairs Forefront*. <https://doi.org/10.1377/hblog20200715.454789>
- [10] Mortell, T.J., Strobel, A.T. (2020). Changes in the office for civil rights enforcement policy on telehealth remote communications in response to COVID-19. *Journal of Pediatric Rehabilitation Medicine*, 13(3): 389-392. <https://doi.org/10.3233/PRM-200760>
- [11] Bhate, C., Ho, C.H., Brodell, R.T. (2020). Time to revisit the Health Insurance Portability and Accountability Act (HIPAA)? Accelerated telehealth adoption during the COVID-19 pandemic. *Journal of the American Academy of Dermatology*, 83(4): e313-e314. <https://doi.org/10.1016/j.jaad.2020.06.989>
- [12] Textor, L., Ventricelli, D., Aronowitz, S.V. (2022). 'Red flags' and 'red tape': Telehealth and pharmacy-level barriers to buprenorphine in the United States. *International Journal of Drug Policy*, 105: 103703. <https://doi.org/10.1016/j.drugpo.2022.103703>
- [13] Indria, D., Alajlani, M., Fraser, H.S. (2020). Clinicians perceptions of a telemedicine system: A mixed method study of Makassar City, Indonesia. *BMC Medical Informatics and Decision Making*, 20(1): 233. <https://doi.org/10.1186/s12911-020-01234-7>
- [14] Hyder, M.A., Razzak, J. (2020). Telemedicine in the United States: An introduction for students and residents. *Journal of Medical Internet Research*, 22(11): e20839. <https://doi.org/10.2196/20839>
- [15] Wang, Y., Qiu, T., Zhou, J., Francois, C., Toumi, M. (2021). Which criteria are considered and how are they evaluated in health technology assessments? A review of methodological guidelines used in western and Asian countries. *Applied Health Economics and Health Policy*, 19(3): 281-304. <https://doi.org/10.1007/s40258-020-00634-0>
- [16] Stefanicka-Wojtas, D., Kurpas, D. (2022). eHealth and mHealth in chronic diseases—Identification of barriers, existing solutions, and promoters based on a survey of EU stakeholders involved in Regions4PerMed (H2020). *Journal of Personalized Medicine*, 12(3): 467. <https://doi.org/10.3390/jpm12030467>
- [17] Bell, A., Khan, M., Sibir, L., Soanes, T., Tran, T. (2025). Ameliorating placement poverty: Insights from OECD countries. *Journal of Higher Education Policy and Management*, 47(3): 299-316.

- <https://doi.org/10.1080/1360080X.2025.2469356>
- [18] Mathew, J., Wesarat, P.O. (2021). Linking ethical standards for healthcare professionals with Indian cultural values. *Asia Pacific Journal of Health Management*, 16(3): 49-58. <https://doi.org/10.24083/apjhm.v16i3.965>
- [19] Taylor, A. (2021). Telemedicine services in Australia and Brazil. In *Healthcare Technology in Context*, pp. 81-119. https://doi.org/10.1007/978-981-16-4075-9_5
- [20] Schofield, M. (2021). Regulatory and legislative issues on telehealth. *Nutrition in Clinical Practice*, 36(4): 729-738. <https://doi.org/10.1002/ncp.10740>
- [21] Bassan, S. (2020). Data privacy considerations for telehealth consumers amid COVID-19. *Journal of Law and the Biosciences*, 7(1): Isaa075. <https://doi.org/10.1093/jlb/Isaa075>
- [22] Pandya, A., Waller, M., Portnoy, J.M. (2022). The regulatory environment of telemedicine after COVID-19. *The Journal of Allergy and Clinical Immunology: In Practice*, 10(10): 2500-2505. <https://doi.org/10.1016/j.jaip.2022.07.001>
- [23] Kaplan, B. (2022). Ethics, guidelines, standards, and policy: Telemedicine, COVID-19, and broadening the ethical scope. *Cambridge Quarterly of Healthcare Ethics*, 31(1): 105-118. <https://doi.org/10.1017/S0963180121000852>
- [24] de Oliveira Andrade, A., Soares, A.B., de Andrade Palis, A., et al. (2022). On the use of telemedicine in the context of COVID-19: Legal aspects and a systematic review of technology. *Research on Biomedical Engineering*, 38(1): 209-227. <https://doi.org/10.1007/s42600-021-00133-8>
- [25] Mazzuca, D., Borselli, M., Gratteri, S., Zampogna, G., Feola, A., Della Corte, M., Guarna, F., Scordia, V., Giannaccare, G. (2022). Applications and current medico-legal challenges of telemedicine in ophthalmology. *International Journal of Environmental Research and Public Health*, 19(9): 5614. <https://doi.org/10.3390/ijerph19095614>
- [26] Orsayeva, R., Berestova, A., Krasilnikova, V., Timoshin, A. (2025). Telemedicine during COVID-19: Features of legal regulation in the field of administrative liability for errors committed by medical institutions. *Egyptian Journal of Forensic Sciences*, 15(1): 26. <https://doi.org/10.1186/s41935-025-00443-3>
- [27] Houser, S.H., Flite, C.A., Foster, S.L. (2023). Privacy and security risk factors related to telehealth services—A systematic review. *Perspectives in Health Information Management*, 20(1). <https://pubmed.ncbi.nlm.nih.gov/37215337/>.
- [28] Aneja, J., Arora, S. (2021). Telemedicine and ethics: Opportunities in India. *Indian Journal of Medical Ethics*, 6(4): 314-320. <https://doi.org/10.20529/IJME.2021.042>
- [29] Baumes, A., Čolić, M., Araiba, S. (2020). Comparison of telehealth-related ethics and guidelines and a checklist for ethical decision making in the midst of the COVID-19 pandemic. *Behavior Analysis in Practice*, 13(4): 736-747. <https://doi.org/10.1007/s40617-020-00475-2>
- [30] Intan Sabrina, M., Defi, I.R. (2021). Telemedicine guidelines in South East Asia—A scoping review. *Frontiers in Neurology*, 11: 581649. <https://doi.org/10.3389/fneur.2020.581649>
- [31] Misheva, K., Ampovska, M. (2022). The legal aspects of telehealth. *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 6: 393-409. <https://doi.org/10.25234/ecllc/22436>
- [32] Al-Alawy, K., Moonesar, I.A. (2023). Perspective: Telehealth—beyond legislation and regulation. *SAGE Open Medicine*, 11: 20503121221143223. <https://doi.org/10.1177/20503121221143223>
- [33] Gallese Nobile, C. (2023). Legal aspects of the use of artificial intelligence in telemedicine. *Journal of Digital Technologies and Law*, 1(2): 314-336. <https://doi.org/10.21202/jdtl.2023.13>
- [34] Shachar, C., Engel, J., Elwyn, G. (2020). Implications for telehealth in a postpandemic future: Regulatory and privacy issues. *Jama*, 323(23): 2375-2376. <https://doi.org/10.1001/jama.2020.7943>
- [35] Fields, B.G. (2020). Regulatory, legal, and ethical considerations of telemedicine. *Sleep Medicine Clinics*, 15(3): 409-416. <https://doi.org/10.1016/j.jsmc.2020.06.004>
- [36] Hoffman, D.A. (2020). Increasing access to care: Telehealth during COVID-19. *Journal of Law and the Biosciences*, 7(1): Isaa043. <https://doi.org/10.1093/jlb/Isaa043>
- [37] Silva, A.B., da Silva, R.M., Ribeiro, G.D.R., Guedes, A.C.C.M., Santos, D.L., Nepomuceno, C.C., Caetano, R. (2020). Three decades of telemedicine in Brazil: Mapping the regulatory framework from 1990 to 2018. *PloS One*, 15(11): e0242869. <https://doi.org/10.1371/journal.pone.0242869>
- [38] Sethi, M.I.S., Manjunatha, N., Channaveerachari, N.K., Chakraborty, T., Math, S.B., Andrade, C. (2025). The digital personal data protection act 2023: Implications for mental healthcare practice in India. *Indian Journal of Psychological Medicine*. <https://doi.org/10.1177/02537176251370651>
- [39] Sood, A., Mishra, D., Surya, V., Singh, H., Sundaresan, R., et al. (2025). Challenges and recommendations for enhancing digital data protection in Indian Medical Research and Healthcare Sector. *NPJ Digital Medicine*, 8: 48. <https://doi.org/10.1038/s41746-025-01448-x>
- [40] Suwadi, P., Ayuningtyas, P.W., Septiningrum, S.Y., Manthovani, R. (2024). Legal comparison of the use of telemedicine between Indonesia and the United States. *International Journal of Human Rights in Healthcare*, 17(3): 315-329. <https://doi.org/10.1108/IJHRH-04-2022-0032>
- [41] Ferorelli, D., Nardelli, L., Spagnolo, L., Corradi, S., et al. (2020). Medical legal aspects of telemedicine in Italy: Application fields, professional liability and focus on care services during the COVID-19 health emergency. *Journal of Primary Care & Community Health*, 11: 2150132720985055. <https://doi.org/10.1177/2150132720985055>
- [42] Faget, K., Lacktman, N.M., Joseph, J., Shalom, A. (2021). Telehealth legal and regulatory issues. In *Telemedicine*, pp. 15-31. https://doi.org/10.1007/978-3-030-64050-7_2
- [43] Scott, R.E., Morris, C., Mars, M. (2021). Development of a “cellphone stewardship framework”: Legal, regulatory, and ethical issues. *Telemedicine and e-Health*, 27(3): 316-322. <https://doi.org/10.1089/tmj.2020.0048>
- [44] Raveesh, B.N., Munoli, R.N. (2020). Ethical and legal aspects of telepsychiatry. *Indian Journal of Psychological Medicine*, 42(5_suppl): 63S-69S. <https://doi.org/10.1177/0253717620962033>

- [45] Zhang, A., Balles, J.A., Henningfield, M.F., Nyland, J.E., Nguyen, T.H., Zgierska, A.E. (2024). Offering recovery rather than punishment: Implementation of a law enforcement-led pre-arrest diversion-to-treatment program for adults with substance use disorders. *Journal of Substance Use and Addiction Treatment*, 159: 209274. <https://doi.org/10.1016/j.josat.2023.209274>
- [46] Montelongo, A., Becker, J.L., Roman, R., de Oliveira, E.B., Umpierre, R.N., Goncalves, M.R., Silva, R., Doniec, K., Yetisen, A.K. (2021). The management of COVID-19 cases through telemedicine in Brazil. *PLoS One*, 16(7): e0254339. <https://doi.org/10.1371/journal.pone.0254339>
- [47] McLean, T.R., McLean, A.B. (2008). Hageseth's principle of extraterritorial jurisdiction and international telemedicine. *Journal of Telemedicine and Telecare*, 14(6): 282-284. <https://doi.org/10.1258/jtt.2008.080416>
- [48] Kuszler, P.C. (1999). Telemedicine and integrated health care delivery: Compounding malpractice liability. *American Journal of Law & Medicine*, 25(2-3): 297-326. <https://doi.org/10.1017/S0098858800010923>
- [49] Mustafa, A., Ahmad, A., Qureshi, A.A., Naseem, A., et al. (2024). Telemedicine practice: Current challenges of consent and autonomy, patient privacy and data security worldwide. *Journal of Society of Prevention, Advocacy and Research King Edward Medical University*, 3(1): 47-53. <https://doi.org/10.21649/jspark.v3i1.360>
- [50] Alsabi, H., Saadon, M.S.I., Othman, M.R., Mohammad, A.M. (2023). The moderation role of innovation and infrastructure on the relationship between COVID-19 crises and health care performance: Evidence from Jordan. *International Journal of Sustainable Development and Planning*, 18(4): 1235-1243. <https://doi.org/10.18280/ijstdp.180428>
- [51] Aakanksha, T., Krishna, B.C. (2025). Security and cybersecurity risk management in e-health systems: A hybrid approach. *International Journal of Safety and Security Engineering*, 15(8): 1603-1610. <https://doi.org/10.18280/ijssse.150806>
- [52] Silverman, R.D. (2000). Regulating medical practice in the cyber age: Issues and challenges for state medical boards. *American Journal of Law & Medicine*, 26(2-3): 255-276. <https://doi.org/10.1017/S0098858800011084>
- [53] Nittari, G., Khuman, R., Baldoni, S., Pallotta, G., Battineni, G., Sirignano, A., Amenta, F., Ricci, G. (2020). Telemedicine practice: Review of the current ethical and legal challenges. *Telemedicine and e-Health*, 26(12): 1427-1437. <https://doi.org/10.1089/tmj.2019.0158>
- [54] Stoll, J., Sadler, J.Z., Trachsel, M. (2020). The ethical use of telepsychiatry in the Covid-19 pandemic. *Frontiers in psychiatry*, 11: 665. <https://doi.org/10.3389/fpsy.2020.00665>
- [55] Imberti, J.F., Tosetti, A., Mei, D.A., Maisano, A., Boriani, G. (2021). Remote monitoring and telemedicine in heart failure: Implementation and benefits. *Current Cardiology Reports*, 23(6): 55. <https://doi.org/10.1007/s11886-021-01487-2>
- [56] Coleman, A., Herselman, M.E., Coleman, M. (2019). Improving computer-mediated synchronous communication of doctors in rural communities through cloud computing: A case study of rural hospitals in South Africa. *The Oriental Anthropologist: A Bi-Annual International Journal of the Science of Man*, 13(1): 23-34. <https://doi.org/10.1177/0976343020130103>