Original Article

law& pass International Journal of Law, Public Administration and Social Studies https://lawpass.org

https://doi.org/10.47353/lawpass.v3i4.133

AI-Driven Healthcare and the Limits of Medical Liability: Rethinking Patient Rights and Legal Accountability in Türkiye and the European Union

Sibel Çimen
Fırat University, Turkey
*Corresponding author: scimen@firat.edu.tr

Abstract

Artificial intelligence (AI) is increasingly used in diagnosis, clinical decision support, patient monitoring, and treatment planning, but its integration complicates the allocation of legal responsibility when patients are harmed. This article examines whether the legal frameworks of Türkiye and the European Union adequately protect patients where clinical decisions are shaped by AI systems. Using comparative doctrinal legal analysis, it evaluates professional negligence, institutional duties, product liability, data protection, informed consent, and evidentiary barriers. It argues that physician-centred liability is insufficient when relevant knowledge, control, and preventive capacity are distributed among clinicians, healthcare institutions, technology providers, and regulators. The article develops the Distributed Accountability Framework for AI-Driven Healthcare (DAF-AIH), which maps responsibility across four dimensions—clinical, institutional, technological, and regulatory—and identifies meaningful human oversight, patient-centred transparency, and effective access to evidence as cross-cutting safeguards. The framework does not create automatic collective liability; it offers a structured method for tracing legally relevant duties, control, omissions, and causal contribution. The comparison highlights both the regulatory resources and unresolved remedial gaps in Türkiye and the EU.

Keywords: artificial intelligence; medical liability; patient rights; legal accountability; healthcare regulation.

Introduction

Artificial intelligence (AI) is moving from experimental settings into routine healthcare. Clinical applications include image interpretation, risk prediction, triage, decision support, remote monitoring, and the generation or summarisation of clinical records. These systems can improve speed, consistency, and access to specialist knowledge, but their outputs are not detached from the legal and institutional conditions in which they are developed and used. An inaccurate recommendation may reflect defective design, unrepresentative training data, inadequate validation, poor integration into a clinical workflow, over-reliance by a practitioner, or the failure to monitor performance after deployment. The legal question is therefore not simply whether a

Received: August 12, 2026 | **Revised:** Sept 27, 2026 | **Accepted:** Oct 13, 2026 | **Publication:** Oct 31, 2026

Copyright (c) 2026 Sibel Çimen
Creative Commons Attribution 4.0 International License.

physician made an error, but how duties and causal contributions should be identified across a sociotechnical chain (Topol, 2019; Morley et al., 2020; WHO, 2021).

Healthcare AI challenges conventional liability because the knowledge needed to understand an adverse outcome is often distributed. A clinician may see an output without knowing how the model was trained or validated. A hospital may purchase a system without having the technical capacity to independently assess its limitations. A developer may control model documentation, update schedules, and performance data, while a patient may not even know that an algorithm materially influenced the decision. This asymmetry can make the injured patient the least informed participant in the process, despite being the person who bears the consequences. Research on medical AI liability has accordingly identified physicians, healthcare institutions, and developers as distinct but potentially overlapping sites of responsibility (Price, Gerke, & Cohen, 2024; Mello & Guha, 2024).

The issue is not that traditional legal doctrines have become irrelevant. Negligence, contractual liability, product liability, informed consent, data protection, and institutional duties remain essential. The difficulty is that each doctrine addresses only part of the problem. A negligence analysis may focus on the clinician's conduct while overlooking the institution's procurement and training decisions. Product liability may address a defective system but not negligent clinical reliance on an otherwise safe product. Data-protection law may regulate the processing of health data without resolving compensation for bodily injury. A fragmented approach risks leaving gaps between the actors and legal regimes involved (Bottomley & Thaldar, 2023; Cestonaro et al., 2023).

International governance instruments provide important normative direction. The World Health Organization identifies human autonomy, safety, transparency, accountability, inclusiveness, and sustainability as principles for AI in health (WHO, 2021). The Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law likewise situates AI governance within human-rights safeguards (Council of Europe, 2024). The OECD AI Principles and UNESCO Recommendation on the Ethics of AI further provide widely used normative benchmarks for trustworthy, human-centred governance (OECD, 2019; UNESCO, 2021). Yet ethical principles and regulatory compliance do not, by themselves, determine who must compensate a patient, what standard of care applies, or how a claimant can obtain evidence held by a provider or manufacturer. Governance and liability are connected, but they perform different legal functions.

The European Union (EU) has developed a layered framework relevant to healthcare AI. The General Data Protection Regulation (GDPR) governs the processing of personal data, including health data. The Medical Devices Regulation (MDR) applies where software meets the definition of a medical device and establishes safety and conformity requirements. The AI Act, as amended by Regulation (EU) 2026/1744, introduces risk-based obligations for covered AI systems, including certain systems used as safety components of regulated medical devices; the 2026 amendment also revises implementation arrangements and timelines. The revised Product Liability Directive (EU) 2024/2853 expressly includes software within the product-liability framework, but its new regime applies to products placed on the market or put into service after

9 December 2026. Importantly, the proposed AI Liability Directive was withdrawn in 2025 and must not be described as enacted or pending legislation (European Parliament & Council, 2016, 2017, 2024a, 2024b; European Parliament, 2025).

Türkiye provides a valuable comparative setting. Its Constitution recognises the state's responsibility to regulate and supervise health services; Law No. 1219 regulates the practice of medicine; the Turkish Code of Obligations (Law No. 6098) supplies general contractual and tort principles; Law No. 6698 governs personal-data processing; and the Regulation on Patient Rights protects information, consent, dignity, and related patient interests. The Medical Device Regulation published in the Official Gazette on 2 June 2021 also provides a sectoral framework relevant to software that qualifies as a medical device. These instruments can apply to AI-assisted healthcare even though they do not constitute a single, comprehensive AI-medical-liability statute (Republic of Türkiye, 1982, 1928, 1998, 2011, 2016, 2021).

The comparison must not collapse regulatory convergence into legal identity. EU regulations apply according to their own territorial and material scope; they do not automatically govern every Turkish healthcare provider or AI deployment. They may nevertheless provide a comparative benchmark, particularly where Turkish medical-device regulation reflects or aligns with EU standards. The analysis therefore distinguishes direct legal application from domestic legal obligations, regulatory alignment, and persuasive comparative lessons.

Existing scholarship has examined medical negligence, product liability, algorithmic opacity, and ethical governance. Mello and Guha (2024) analyse malpractice risks arising from healthcare AI tools; Price, Gerke, and Cohen (2024) map liability across clinicians, institutions, and developers; Bottomley and Thaldar (2023) explain the conceptual difficulties of assigning liability for healthcare AI harm; Gerke et al. (2020) analyse ethical and legal challenges in AI-driven healthcare, and Cestonaro et al. (2023) review medical liability in AI-supported diagnosis. The contribution advanced here is deliberately narrower than a claim to be the first study of AI and medical liability. It is an integrated comparative legal model that connects the allocation of responsibility to patient-facing safeguards and the practical ability to establish a claim across Türkiye and the EU.

This article addresses four questions: (1) how far do the legal frameworks of Türkiye and the EU address injury arising from AI-assisted healthcare; (2) how should legal responsibility be assessed among clinicians, healthcare institutions, technology providers, and public regulators; (3) how do opacity, causation, and unequal access to technical evidence affect patients' ability to obtain a remedy; and (4) what safeguards can make accountability effective without imposing automatic liability on every actor involved? It argues that responsibility should be allocated by reference to the duty owed, the actor's control and knowledge, the foreseeability of the risk, the capacity to prevent or mitigate harm, and the actor's causal contribution.

The article's principal contribution is the Distributed Accountability Framework for AI-Driven Healthcare (DAF-AIH). The framework distinguishes four dimensions of responsibility—clinical, institutional, technological, and regulatory—and overlays them with three safeguards: meaningful human oversight, patient-centred transparency, and effective access to evidence. It does not treat AI as a legal person, create strict liability by implication, or presume

that every participant is jointly liable. Rather, it offers a structured way to identify the legally relevant actor, duty, omission, and causal contribution in a particular case. This approach is intended to connect the governance of AI systems with the patient's right to explanation, review, and effective redress.

Method

This study adopts doctrinal legal research combined with functional comparative analysis. The doctrinal component interprets primary legal materials governing medical practice, patient rights, personal data, medical devices, AI systems, and civil liability in Türkiye and the European Union. The Turkish analysis focuses on the Constitution, Law No. 1219, Law No. 6098, Law No. 6698, the Regulation on Patient Rights, and the Medical Device Regulation. The EU analysis examines the GDPR, the MDR, the AI Act, and Directive (EU) 2024/2853 on liability for defective products.

The comparative component evaluates how each system addresses five connected issues: the standard of professional care; the duties of healthcare institutions; the responsibility of developers and manufacturers; patient autonomy and data protection; and access to evidence and causation. Comparison is functional rather than based on an assumption that the two legal systems are identical. EU instruments are treated as binding within their applicable scope and as comparative reference points where they do not directly apply in Türkiye.

Secondary sources comprise peer-reviewed legal, medical, and interdisciplinary scholarship and authoritative institutional guidance, particularly WHO and Council of Europe materials. The DAF-AIH framework is developed through normative synthesis of these materials. No interviews, surveys, case-file dataset, or quantitative assessment was conducted. Accordingly, the article does not make empirical claims about the frequency of AI-related injury, litigation outcomes, or the effectiveness of particular safeguards in practice.

The limits of physician-centred medical liability

Medical negligence remains a central route for assessing harm associated with clinical decision-making. A physician is ordinarily expected to exercise the level of care reasonably required by professional standards and the circumstances of the case. The use of decision-support software does not automatically lower that standard or transfer the physician's professional obligations to a machine. A clinician who blindly follows an obviously inconsistent recommendation, fails to consider relevant symptoms, or uses a tool outside its intended purpose may still be negligent. Conversely, it would be unrealistic to assume that every physician can independently audit a complex model or detect a hidden defect in its training data (Mello & Guha, 2024; Price, Gerke, & Cohen, 2024).

The proper inquiry is contextual. It should consider what information was reasonably available to the clinician, what the system was designed to do, whether the clinician received adequate training, whether the output was presented as advisory or determinative, and whether warning signs required independent judgment. The relevant professional standard should not be

framed as an obligation to understand every technical feature of an AI model. It should require appropriate selection, use, interpretation, and escalation in light of the clinician's role and available information. Professional responsibility is therefore neither displaced by AI nor unlimited by it.

Automation bias creates a further difficulty. Clinicians may overvalue a computer-generated recommendation, particularly when it appears precise or is embedded in routine workflows. At the same time, requiring clinicians to disregard every AI output would deprive patients of potentially beneficial tools. The legal standard should instead distinguish reasonable reliance from unreasonable delegation. Meaningful oversight requires the practical ability to question an output, access relevant clinical information, and depart from a recommendation without institutional penalty. A nominal human sign-off is insufficient where the clinician lacks time, authority, or competence to review the result (WHO, 2021; Cestonaro et al., 2023).

Institutional responsibility: procurement, integration, and supervision

Healthcare institutions are not passive venues in which individual clinicians happen to use AI. Hospitals and health providers decide whether to acquire a system, which clinical tasks it will support, how it will be integrated into workflows, what staff training will be provided, and how performance will be monitored. Those decisions can create or amplify risks independently of the clinician's conduct. Institutional responsibility may therefore arise where a provider deploys an inadequately validated system, fails to assess suitability for its patient population, provides insufficient training, ignores recurring incidents, or does not maintain procedures for escalation and review. Operational risk-management approaches, including the NIST AI Risk Management Framework, can support this governance process by structuring the identification, measurement, management, and monitoring of AI risks, although such voluntary guidance does not replace legal duties (National Institute of Standards and Technology, 2023).

The institution's duty is particularly important because the hospital often acts as the bridge between the developer and the clinician. It may be the party best positioned to demand technical documentation, negotiate contractual assurances, verify local performance, and preserve audit logs. The institution should assess whether the system is appropriate for the intended purpose and local setting, whether its limitations are communicated, and whether staff can identify circumstances in which the output should not be relied upon. This is consistent with the broader view that accountability in healthcare AI requires governance at the organisational level, not only individual professional ethics (Reddy et al., 2020; WHO, 2021).

In Türkiye, institutional duties should be analysed through the applicable rules on healthcare provision, patient rights, medical devices, contractual obligations, and general liability. In the EU, the AI Act and MDR may impose relevant provider or deployer obligations depending on the system's classification, intended purpose, and role in a regulated medical device. These regulatory duties can inform the assessment of reasonable institutional conduct, but regulatory non-compliance and civil liability remain analytically distinct. A breach may be

relevant evidence of fault or defect, yet a claimant must still establish the elements required by the applicable cause of action.

Institutions should consequently maintain an AI governance process that covers pre-deployment assessment, role allocation, staff competence, clinical validation, monitoring, incident response, and periodic reassessment. This is not a claim that every hospital must build its own technical audit laboratory. Rather, institutions should possess sufficient expertise—internally or through independent support—to make an informed decision about deployment and to know when specialist scrutiny is required.

Technological responsibility and product liability

Developers and manufacturers control important stages of the AI lifecycle, including system design, training and validation, documentation, warnings, cybersecurity, maintenance, and updates. Liability may arise where a system is defective, inadequately tested, misleadingly marketed, or insufficiently accompanied by instructions and warnings. It may also arise under contractual or other national rules where the relevant elements are established. The fact that an AI system is complex or adaptive does not make it legally immune; it does, however, complicate the assessment of defect, foreseeability, and causation (Bottomley & Thaldar, 2023; Price, Gerke, & Cohen, 2024).

The EU's revised Product Liability Directive is significant because it expressly treats software, including AI systems, as a product for the purposes of the new no-fault product-liability regime. It also responds to evidentiary difficulties in technically complex cases through disclosure mechanisms and rebuttable presumptions under specified conditions. However, the Directive's temporal scope matters: it applies to products placed on the market or put into service after 9 December 2026, and Member States must transpose it by that date. At the time of this article's legal assessment, the new regime should therefore be described as adopted legislation with a future application date, not as already governing every AI-related injury (European Parliament & Council, 2024a).

The proposed AI Liability Directive, COM(2022) 496, should not be presented as part of the operative EU legal framework. The European Parliament's legislative observatory records the procedure as withdrawn on 6 October 2025. Its earlier proposals concerning disclosure and presumptions may remain relevant to the policy debate, but they do not create enforceable rights as an enacted directive. This distinction is important because inaccurate descriptions of legislative status can undermine the legal reliability of comparative analysis (European Parliament, 2025).

Product liability is not a complete substitute for medical negligence or institutional responsibility. A product may satisfy safety requirements yet be used negligently in a particular clinical context. Conversely, a clinician may act reasonably while a latent defect or inadequate warning contributes to injury. The legal analysis should therefore avoid forcing all disputes into a single liability category. It should identify whether the alleged failure concerns product design,

manufacture, information, update, clinical use, institutional deployment, or a combination of these.

Patient rights, informed consent, and health-data protection

Patient autonomy requires more than the formal collection of consent to treatment. Where AI materially influences diagnosis, triage, or treatment, patients may need information about the role of the system, the significance of its output, relevant limitations, and the availability of human review. The precise disclosure obligation should be proportionate to the clinical context. A minor administrative use may not require the same explanation as an algorithm that materially shapes a cancer diagnosis or determines access to urgent treatment. The central concern is whether the patient can make an informed decision and retain a meaningful opportunity to question consequential clinical choices.

The WHO guidance places human autonomy, transparency, accountability, and protection of individuals at the centre of health AI governance (WHO, 2021). These principles support a patient-centred interpretation of existing rights, but they do not automatically create a freestanding right to receive source code or a complete technical explanation of every model output. The legal question is what information is necessary for a patient to understand the material role of AI, exercise existing rights, and challenge a decision effectively. Transparency must be practical and intelligible rather than merely technical.

Data protection is a related but distinct dimension. Health data are particularly sensitive, and their processing for AI development or deployment raises questions about lawful basis, purpose limitation, data minimisation, security, retention, and data-subject rights. In the EU, the GDPR provides the principal horizontal framework. Article 22 is relevant to certain decisions based solely on automated processing that produce legal or similarly significant effects, subject to its scope and exceptions; it should not be casually equated with a universal right to human review of every AI-supported clinical judgment. In Türkiye, Law No. 6698 regulates personal-data processing and includes special rules for sensitive personal data, including health data. The 2024 amendments should be considered in their current form and commencement context. The European Commission's Ethics Guidelines for Trustworthy AI similarly treat human agency, technical robustness, privacy, transparency, and accountability as interdependent requirements (European Commission High-Level Expert Group on Artificial Intelligence, 2019).

Consent to treatment and the legal basis for processing personal data should not be conflated. A patient may consent to a medical intervention without thereby giving unrestricted consent to every secondary use of their data for model training, commercial development, or unrelated research. Equally, a lawful basis for data processing does not establish that a treatment decision was clinically reasonable. A sound accountability analysis must keep these legal questions separate while recognising their interaction.

Algorithmic opacity, causation, and access to evidence

One of the most serious barriers to effective redress is evidentiary asymmetry. The patient may know the injury and the clinical outcome but lack access to model logs, version histories, input data, validation reports, system warnings, and records showing how the output influenced the decision. Those materials may be held by the hospital, manufacturer, or software provider. Without them, the claimant may struggle to identify whether the harm arose from a defective model, an inappropriate deployment, an unreasonable clinical decision, or a combination of factors. Algorithmic opacity therefore has procedural consequences: it can make a formally available cause of action practically difficult to pursue (Price, 2018; Wachter et al., 2017; Mello & Guha, 2024).

Causation is also more complex where several conditions contribute to the outcome. A model may produce an inaccurate risk score; a clinician may rely on it; the institution may have failed to validate the system; and the patient's underlying condition may independently affect the outcome. The law should not assume that the AI output was the sole cause merely because it appeared in the clinical record. Nor should causal complexity automatically defeat a claim. Courts can assess the evidence concerning the system's role, the clinical counterfactual, foreseeable use, and the contribution of each alleged breach under the applicable national rules.

Recordkeeping is therefore a substantive accountability safeguard. Healthcare institutions and providers should preserve relevant model versions, inputs and outputs where lawful, timestamps, warnings, user interactions, override decisions, and incident reports. The records should be sufficient to reconstruct the decision without indiscriminately disclosing unrelated patient data or protected security information. Where disclosure is necessary, confidentiality can be protected through controlled access, redaction, expert examination, or judicial supervision. The objective is not unlimited transparency; it is access sufficient to test the claim.

The EU Product Liability Directive 2024/2853 recognises that claimants may face disproportionate difficulties in proving defectiveness or causation in technically or scientifically complex cases and provides mechanisms for disclosure and presumptions under defined conditions. These mechanisms are important, but they are confined to the Directive's scope and do not automatically resolve every medical-negligence or institutional-liability dispute. In Türkiye, the effectiveness of existing procedural and substantive rules should be assessed in light of the claimant's ability to request and evaluate records held by healthcare providers and manufacturers. This is a key area for future doctrinal and procedural clarification.

Comparative assessment: Türkiye and the European Union

The EU framework is comparatively more explicit in its use of risk-based AI regulation and in the integration of AI governance with medical-device and product-safety rules. The AI Act, as amended in 2026, establishes obligations for providers and deployers of covered high-risk systems, while the MDR governs medical devices within its scope and the GDPR regulates personal-data processing. The revised Product Liability Directive adds a modernised route for claims involving defective software, although its new regime applies only from the date specified

in the Directive. These instruments strengthen preventive governance and may improve the evidentiary environment, but they do not create a single, comprehensive code of medical AI liability.

Türkiye's framework relies more heavily on the interaction of general civil-liability principles, professional regulation, patient-rights rules, data-protection law, and medical-device regulation. This does not mean that Turkish law is incapable of addressing AI-related injury. Existing doctrines may apply to negligent clinical conduct, institutional failures, defective products, and unlawful data processing. The challenge is the absence of a clearly integrated statutory architecture that expressly allocates AI-specific duties across the clinical and technological lifecycle. The practical response should therefore focus on clarifying how existing duties apply, improving institutional governance, and ensuring that relevant evidence is retained and accessible.

The comparison reveals three common concerns. First, regulatory compliance is not equivalent to compensation: safety and governance rules may reduce risk but do not, by themselves, establish a patient's civil claim. Secondly, liability remains multi-actor: clinicians, institutions, and technology providers may each control different parts of the risk. Thirdly, patient rights depend on procedural capacity: disclosure, review, record preservation, and access to evidence are necessary if substantive rights are to be enforceable. These concerns support an integrated framework rather than a search for a single actor who can be held responsible in every case. Recent comparative work published in 2026 similarly identifies evidence asymmetry, documentation integrity, multi-actor control, warning and reliance, and causation under uncertainty as persistent difficulties in healthcare AI claims (Tujjar et al., 2026). The present framework extends that claimant-facing analysis by structuring responsibility across four legal dimensions and applying the same architecture comparatively to Türkiye and the EU, with patient-centred safeguards integrated across each dimension.

Regulatory convergence between Türkiye and the EU should be pursued cautiously. EU standards can provide a useful benchmark for medical-device safety, risk management, documentation, and oversight, but transplanting EU categories without regard to Turkish institutional capacity and domestic legal structure would be inappropriate. The more defensible approach is functional adaptation: identify the protective purpose of each EU mechanism, determine whether an equivalent duty exists under Turkish law, and consider whether clarification or reform is needed to close a specific accountability gap.

The Distributed Accountability Framework for AI-Driven Healthcare (DAF-AIH)

The preceding analysis supports a framework that traces responsibility across the stages at which risk is created, controlled, communicated, and capable of being remedied. DAF-AIH is organised around four dimensions. Clinical responsibility concerns professional selection, interpretation, and use of AI outputs. Institutional responsibility concerns procurement, validation, integration, training, supervision, monitoring, and incident response. Technological

responsibility concerns design, testing, documentation, warnings, cybersecurity, maintenance, and updates. Regulatory responsibility concerns the public authority's role in establishing and supervising applicable safety and governance requirements. The dimensions are analytically distinct but may overlap in a single case.

Responsibility should be allocated through five questions: what legal duty applied; which actor had relevant control or knowledge; whether the risk was reasonably foreseeable; whether the actor had a practical capacity to prevent or mitigate it; and whether the breach materially contributed to the injury. This approach avoids two extremes. It rejects physician-only liability where the decisive failure occurred upstream, but it also rejects automatic collective liability merely because several actors participated in the system's lifecycle. Each claim must remain grounded in the elements of the relevant legal cause of action.

Three safeguards operate across all four dimensions. Meaningful human oversight requires adequate competence, access to relevant information, sufficient time, and authority to reject or escalate an AI recommendation. Patient-centred transparency requires proportionate disclosure when AI materially influences care, together with understandable information about limitations and review routes. Effective access to evidence requires preservation and proportionate disclosure of clinical, institutional, and technical records. These safeguards are mutually reinforcing: oversight without information is nominal; transparency without review is weak; and legal rights without evidence may be practically inaccessible.

Table 1. Distributed Accountability Framework for AI-Driven Healthcare (DAF-AIH).

Area of responsibility	Core legal responsibility	Key accountability question
Clinical	Appropriate selection, interpretation, and use of AI outputs; professional judgment; escalation and documentation.	Did the clinician act reasonably in the circumstances and retain meaningful clinical judgment?
Institutional	Procurement, local validation, workflow integration, staff training, supervision, monitoring, and incident response.	Did the provider create and maintain conditions for safe and accountable use?
Technological	Design, testing, data quality, documentation, warnings, cybersecurity, maintenance, and material updates.	Did the developer or manufacturer meet applicable product, contractual, and safety duties?
Regulatory	Rulemaking, conformity and market surveillance, enforcement, and oversight within statutory competence.	Were applicable public safeguards established and effectively supervised?

Cross-cutting safeguards: (1) meaningful human oversight; (2) patient-centred transparency; and (3) effective access to evidence.

Source: Author's normative synthesis.

Conclusion

AI-assisted healthcare does not eliminate the relevance of established legal doctrines, but it exposes the limits of an approach that places primary responsibility on the individual physician. Harm may arise through the interaction of clinical judgment, institutional deployment, technological design, and regulatory oversight. The comparative analysis shows that Türkiye and the European Union possess legal resources capable of addressing important parts of this problem, including professional duties, general civil liability, patient rights, data protection, medical-device regulation, and product liability. However, these resources do not automatically form a coherent system for identifying responsibility and securing redress when AI contributes to patient injury.

This article has proposed the Distributed Accountability Framework for AI-Driven Healthcare (DAF-AIH), which organises responsibility into clinical, institutional, technological, and regulatory dimensions. Its three cross-cutting safeguards—meaningful human oversight, patient-centred transparency, and effective access to evidence—connect preventive governance with the patient's ability to understand and challenge AI-influenced care. The framework is not a strict-liability rule and does not presume that all participants are jointly liable. It is a method for tracing legally relevant duties, control, knowledge, omissions, and causal contribution under the applicable law.

For Türkiye, the analysis supports clearer guidance on institutional AI governance, clinical oversight, patient-facing disclosure, and preservation of technical records, while maintaining the distinction between domestic law and EU regulatory standards. For the EU, the AI Act, MDR, GDPR, and revised Product Liability Directive provide complementary safeguards, but the withdrawal of the proposed AI Liability Directive confirms that civil-liability questions continue to depend substantially on existing national rules and the scope of product-liability law. In both settings, legal compliance should be assessed separately from the patient's entitlement to compensation.

The study is doctrinal and normative; it does not empirically test the framework against litigation files or hospital deployment data. Future research should examine judicial decisions, clinical incident reports, procurement and software contracts, and the practical operation of disclosure and review procedures. Ultimately, the legitimacy of healthcare AI depends not only on technical performance but also on whether responsibility remains identifiable and patients retain meaningful access to information, review, and effective remedies.

AI Disclosure Statement

The author acknowledges the use of AI-assisted tools during the preparation of this manuscript for language refinement, editorial assistance, and improvement of manuscript structure and clarity. The author takes full responsibility for the originality, accuracy, interpretation of legal materials, verification of references, and final content of this article.

References

Bottomley, D., & Thaldar, D. (2023). Liability for harm caused by AI in healthcare: An overview of the core legal concepts. Frontiers in Pharmacology, 14, 1297353. https://doi.org/10.3389/fphar.2023.1297353

Cestonaro, C., Delicati, A., Marcante, B., Caenazzo, L., & Tozzo, P. (2023). Defining medical liability when artificial intelligence is applied on diagnostic algorithms: A systematic review. Frontiers in Medicine, 10, 1305756. https://doi.org/10.3389/fmed.2023.1305756

Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

European Commission High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament and Council of the European Union. (2017). Regulation (EU) 2017/745 on medical devices. Official Journal of the European Union, L 117, 1–175. https://eur-lex.europa.eu/eli/reg/2017/745/oj

European Parliament and Council of the European Union. (2024a). Directive (EU) 2024/2853 on liability for defective products. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2024/2853/oj

European Parliament and Council of the European Union. (2024b). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

European Parliament and Council of the European Union. (2026). Regulation (EU) 2026/1744 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2026/1744/oj

European Parliament. (2025). Procedure 2022/0303(COD): Artificial Intelligence Liability Directive. Legislative Observatory. https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2022/0303(COD)

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28, 689–707. https://doi.org/10.1007/s11023-018-9482-5

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In A. Bohr & K. Memarzadeh (Eds.), Artificial Intelligence in Healthcare (pp. 295–336). Academic Press.

Mello, M. M., & Guha, N. (2024). Understanding liability risk from using health care artificial intelligence tools. The New England Journal of Medicine, 390(3), 271–278. https://doi.org/10.1056/NEJMhle2308901

Morley, J., Machado, C. C. V., Burr, C., Cowls, J., Joshi, I., Taddeo, M., & Floridi, L. (2020). The ethics of AI in health care: A mapping review. Social Science & Medicine, 260, 113172. https://doi.org/10.1016/j.socscimed.2020.113172

National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

OECD. (2019). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Price, W. N., II, Gerke, S., & Cohen, I. G. (2024). Liability for use of artificial intelligence in medicine. In B. Solaiman & I. G. Cohen (Eds.), Research Handbook on Health, AI and the Law. Edward Elgar Publishing. https://doi.org/10.4337/9781802205657.ch09

Price, W. N., II. (2018). Big data and black-box medical algorithms. Science Translational Medicine, 10(471), eaao5333. https://doi.org/10.1126/scitranslmed.aao5333

Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2020). A governance model for the application of AI in health care. Journal of the American Medical Informatics Association, 27(3), 491–497. https://doi.org/10.1093/jamia/ocz192

Republic of Türkiye. (1928). Law No. 1219 on the Practice of Medicine and Medical Sciences.

Republic of Türkiye. (1982). Constitution of the Republic of Türkiye. Official Gazette No. 17863 (Repeating), 9 November 1982.

Republic of Türkiye. (1998). Regulation on Patient Rights. Official Gazette No. 23420, 1 August 1998.

Republic of Türkiye. (2011). Law No. 6098, Turkish Code of Obligations. Official Gazette No. 27836, 4 February 2011.

Republic of Türkiye. (2016). Law No. 6698 on the Protection of Personal Data. Official Gazette No. 29677, 7 April 2016. https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law

Republic of Türkiye. (2021). Medical Device Regulation. Official Gazette No. 31499, 2 June 2021.

Topol, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine, 25, 44–56. https://doi.org/10.1038/s41591-018-0300-7

Tujjar, O., Ientile, G., & Toppetti, F. (2026). After the AI Liability Directive: Civil liability for healthcare AI and the limits of EU risk regulation. European Journal of Risk Regulation, First View, 1–18. https://doi.org/10.1017/err.2026.10130

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005

World Health Organization. (2021). Ethics and governance of artificial intelligence for health: WHO guidance. https://www.who.int/publications/i/item/9789240029200

World Medical Association. (2022). WMA International Code of Medical Ethics. https://www.wma.net/policies-post/wma-international-code-of-medical-ethics/