Thresholds of agency in medical artificial intelligence: A liability framework for healthcare professionals under European Union law

M. Ampovska

Goce Delcev University,
10, Krste Misirkov str., Stip, 2000, Republic of North Macedonia

For citation: Ampovska, M. 2026. "Thresholds of agency in medical artificial intelligence: A liability framework for healthcare professionals under European Union law". *Vestnik of Saint Petersburg University. Law* 1: 109–127. EDN LUWFEI

The rapid integration of sophisticated artificial intelligence (AI) into clinical practice represents a paradigm shift for healthcare, fundamentally challenging traditional conceptions of medical liability and demanding a new legal framework. This article confronts this challenge by proposing a novel "Threshold Typology" to systematically analyze the liability of healthcare professionals within the European Union's complex and multi-layered regulatory environment. We argue that the question of liability is not monolithic but turns on which of three distinct thresholds of agency a professional cross. The analysis first delineates the Regulatory Threshold, established by the preventive and ex-ante obligations of the Artificial Intelligence Act (AI Act), the General Data Protection Regulation (GDPR), and the Medical Device Regulation (MDR). This threshold focuses on compliance with duties of risk management, human oversight, data governance, and vigilance, where breaches can inform subsequent liability determinations. The Professional Threshold is then examined, defined by the fault-based standards of national malpractice law, which are procedurally adapted by the proposed AI Liability Directive (AILD) through mechanisms like disclosure of evidence and rebuttable presumptions of causality. Finally, the Product Threshold is explored, grounded in the strict liability regime of the revised Product Liability Directive (rPLD), which becomes directly relevant when healthcare professionals substantially modify AI systems, effectively transitioning into the role of a producer. By meticulously dissecting the interplay between these five core EU instruments: the AI Act, the AILD, the rPLD, the GDPR, and the MDR, this article provides an indispensable doctrinal map. It demonstrates that liability is contingent, distributed, and highly context-specific, depending on whether the professional acts as a user, an overseer, or a modifier of the AI system. The Threshold Typology thus serves as a vital analytical tool, translating a fragmented legal architecture into a coherent and operational framework for legal scholars, practitioners, and healthcare professionals, while signaling a broader shift from reactive compensation towards a proactive governance of medical AI.

Keywords: medical artificial intelligence liability, European Union artificial intelligence law, healthcare professionals, threshold of agency, product liability directive, duty of care, strict liability, fault liability.

1. Introduction

The increasing use of artificial intelligence (AI) in healthcare exposes healthcare professionals to novel liability challenges, requiring an analysis that situates their responsibility within the evolving European Union (EU) regulatory framework. Unlike other domains of professional practice, clinical decision-making is already subject to strict standards of

diligence, oversight, and accountability. Previous research highlights persistent uncertainty surrounding opacity, accountability, and responsibility in the use of AI systems for clinical decision-making. In particular, the opacity of such systems complicates the allocation of responsibility between developers and healthcare professionals, underscoring the need for clearer legal analysis to define obligations and liability in cases of patient harm (Smith 2021, 544). This notion, combined with the spread of AI-enabled healthcare systems, highlights the need to map how EU regulatory, product, and professional liability rules interact to define the conditions under which healthcare professionals may be held liable.

At the centre of this framework stand five EU instruments that together structure the liability environment: the Artificial Intelligence Act (AI Act)[1], the revised Product Liability Directive (rPLD)[2], the proposed AI Liability Directive (AILD)[3], the General Data Protection Regulation (GDPR)[4] and the Medical Device Regulation (MDR)[5]. These instruments jointly determine the obligations of providers, deployers, and users of medical AI, while also influencing how liability is attributed when harm occurs. Other legal sources, such as national patient rights laws or sector-specific malpractice provisions, also affect liability. However, for this research, the focus remains on these five EU-level instruments, since they directly regulate the preventive, procedural, and substantive bases of liability in medical AI[6]. To analyze how these instruments shape liability for healthcare professionals, this paper employs a doctrinal legal research methodology. Doctrinal analysis is used to interpret legislative texts and proposals while engaging with scholarly commentary to evaluate their adequacy and coherence. The aim is not only to describe obligations, but to identify thresholds at which healthcare professionals may cross from regulatory compliance into liability.

For this purpose, a threshold typology is developed, distinguishing three dimensions: 1) Regulatory Thresholds, based on preventive obligations of risk management, transparency, oversight, and data governance imposed by the AI Act, GDPR, and MDR; 2) Professional Thresholds, defined by fault-based liability standards under national malpractice law, complemented by the procedural innovations of the AILD, such as presumptions of causality and access to evidence; 3) Product Thresholds, grounded in the PLD, which extends strict liability to AI-enabled medical products and assigns responsibility to those who substantially modify certified devices (see Table 1).

This typology allows for a systematic analysis of when and how healthcare professionals may be held liable for harms involving AI. Regulatory thresholds capture ex ante duties of diligence, professional thresholds link AI use to the duty of care under malprac-

[1] Artificial Intelligence Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts, OJ L 168, 1–108.

[2] Product Liability Directive (Revised), Directive (EU) 2024/1799 of the European Parliament and of the Council of June 13, 2024 on liability for defective products (recast), OJ L 182, 1–41.

[3] AI Liability Directive Proposal, European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final, Brussels, September 28, 2022.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, General Data Protection Regulation, OJ L 119, 04.05.2016, 1–88.

[5] Regulation (EU) 2017/745 of the European Parliament and of the Council of April 5, 2017, Medical Device Regulation, OJ L 117, 05.05.2017, 1–175.

[6] Although recent EU legislative developments have significantly expanded the regulation of AI, a systematic analysis of how this body of law applies in the healthcare context remains largely absent (Schmidt et al. 2024, 2).

Table 1. **Analytical thresholds for liability of healthcare professionals using AI**

Threshold	Legal Source(s)	Doctrinal Focus
Regulatory Threshold	Artificial Intelligence Act; Medical Device Regulation; General Data Protection Regulation	Compliance with oversight duties, conformity assessment, documentation, and data governance as preventive obligations informing liability.
Professional Threshold	National tort/malpractice law; AI Liability Directive Proposal	Standard of care, diligence, and the role of evidentiary presumptions in allocating fault-based liability.
Product Threshold	The Revised Product Liability Directive	Strict liability for defective products and liability of healthcare professionals as de facto modifiers when altering certified devices.

tice law, and product thresholds clarify liability where healthcare professionals act as de facto modifiers of AI-enabled devices. Together, these dimensions reveal that liability is neither exclusively regulatory nor purely professional, but rather layered, reflecting the intersection of EU harmonisation and national discretion.

The scope of the study is limited to EU instruments, with national malpractice law considered only insofar as it interacts with EU liability proposals. This reflects the current state of harmonisation: while the PLD and AI Act impose clear preventive and product-level obligations, fault-based liability remains primarily national, with the AILD still under negotiation. The analysis therefore combines textual interpretation of EU legal instruments with academic commentary, in order to clarify how liability thresholds are emerging for healthcare professionals using AI systems. Given the regulatory focus and space limitations, other important dimensions of analysis, such as judicial practice and empirical evidence, are acknowledged but remain outside the scope of this paper.

2. Basic research

2.1. EU Liability Architecture for AI in Healthcare

This section serves as a legal map, outlining the main EU instruments that together structure the liability landscape for healthcare professionals using AI, and providing the foundation for the threshold-based analysis developed in the following part of the paper. The liability of healthcare professionals using AI, as already mentioned, is embedded in a multi-layered framework of EU instruments. Taken together, the AI Act, the revised PLD, the proposed AILD, GDPR, and the MDR, create an architecture that blends preventive obligations, strict product rules, and adapted fault-based liability.

The AI Act, proposed in 2021 after preparatory work by the High-Level Expert Group on AI, adopted on March 13, 2024 by the European Parliament and entered into force on August 1, 2024, forms a central element of the EU's digital policy strategy, seeking to establish a safe and trustworthy ecosystem for AI that balances innovation with the protection of fundamental rights. Adopted as a directly applicable regulation, it introduces a horizontal, risk-based framework that applies uniformly across sectors, including healthcare, with obligations calibrated to the level of risk posed by different AI systems (Kolfschooten,

van Oirschot 2024, 2). The AI Act applies comprehensively to digital medical products, covering AI-enabled medical devices, diagnostics, and regulated clinical decision-support tools, whether stand-alone software or hardware–software combinations. These products already fall under the MDR and the In Vitro Diagnostic Regulation (IVDR)[7], which impose strict sectoral compliance requirements, and they must also comply with the GDPR when processing personal health data (Aboy, Minssen, Vayena 2024, 2).

The AI Act prohibits AI practices deemed to present unacceptable risks and subjects high-risk systems, such as AI-enabled medical devices or diagnostic tools, to stringent requirements, including risk management, data governance, and human oversight. In healthcare, these obligations apply to medical devices of specific risk class, which must undergo third-party conformity assessment under the MDR, with the AI Act adding an additional regulatory layer by integrating AI-specific safeguards into existing device certification procedures (Kolfschooten, van Oirschot 2024, 4–5).

The rPLD establishes a harmonised EU-level regime of strict liability for defective products. It addresses substantive and procedural aspects of product liability, focusing on harm to life, health, property, and data, with claims directed primarily against manufacturers and other actors in the supply chain (Hacker 2023, 7). At the same time, the rPLD modernises EU product law by extending strict liability to AI-enabled goods and software and by aligning its scope with the AI Act's risk classification, thereby creating a bridge between AI regulation and product-safety law. Complemented by the proposed AILD, which translates breaches of AI Act duties into procedural presumptions in fault-based claims, the rPLD helps knit together preventive regulation, product strict liability and national negligence regimes, producing a compact but only partially harmonised EU liability architecture (Ballell 2023, 250).

When it comes to AILD, it should be emphasized that it remains at a provisional stage as a legislative proposal, with its enforceability contingent on formal adoption and subsequent national transposition within the prescribed timelines (Art. 1 (4), Recital 11), rather than operating as immediately binding law. At this point, the AILD proposal functions as a procedural complement to existing national tort laws, aiming to ease evidentiary barriers in fault-based claims involving AI systems. It introduces rebuttable presumptions of causation and disclosure obligations, potentially covering not only traditional harms but also infringements of fundamental rights and financial loss, while leaving substantive liability standards to Member States (Hacker 2023, 7). The explanatory memorandum to the AILD highlights that existing national fault-based liability regimes are ill-suited to address the challenges posed by AI systems, given their opacity, autonomy, and complexity[8]. By situating liability as one of the main barriers to AI uptake in the internal market, the proposal reflects the Commission's broader strategy to foster trust and ensure that injured parties are not left without effective avenues of redress. The AILD proposal aims

[7] Regulation (EU) 2017/746 of the European Parliament and of the Council of April 5, 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU. OJ, L 117, 176–332.

[8] It has been recognized that no Member State currently provides liability frameworks specifically designed for AI outside of narrow contexts such as automated vehicles. Damages caused by AI must therefore be compensated under traditional liability regimes, whether fault-based or risk-based. This results in fragmentation, as national approaches differ with respect to standards of proof, burden of causation, and the scope of risk-based liability. Identical AI systems may therefore give rise to differing legal outcomes across Member States (Ampovska 2024, 466–467).

to adapt non-contractual liability rules to AI's distinctive characteristics. It does so primarily through procedural innovations: presumptions of causality where fault is plausible but difficult to prove, and disclosure obligations addressing information asymmetries between victims and deployers[9]. It has been concluded that the AILD proposal although adaptive and forward-looking, offers only minimal harmonization because it is structured as directives. While it aims to establish uniform principles, the reliance on Member State transposition leaves room for divergent outcomes, particularly in the field of fault-based liability (Ampovska 2024). Still, by codifying presumptions, the AILD fortifies the professional threshold, directly linking liability to failures of oversight and diligence.

The GDPR adds a transversal layer of obligations, embedding principles of transparency, accountability, and lawful processing of sensitive health data. These duties extend to actors deploying AI, shaping the environment in which healthcare professionals interact with algorithmic systems (Bagave et al. 2025, 10–11). Violations not only attract regulatory sanctions but also influence fault-based liability analyses by redefining what constitutes duty of care in data-intensive contexts. Since AI in healthcare often processes sensitive patient data, liability of health healthcare professionals may also intersect with GDPR compliance. Improper handling or insufficient safeguarding of health data in AI-assisted treatment could expose professionals to liability under data protection law (Schmidt et al. 2024).

The MDR consolidates previous directives into a single framework, establishing high standards of safety, quality, and transparency for medical devices while supporting innovation and harmonising market rules across the EU. It reinforces key elements such as conformity assessment, clinical investigations, vigilance, and traceability, ensuring reliable data and patient protection, including for devices incorporating AI, and aligning with international guidance to facilitate regulatory convergence.

Taken together, these EU instruments establish a layered liability architecture that blends regulatory oversight, product safety, and duty of care. The AI Act and MDR define the standards and compliance obligations for AI-enabled medical devices, the rPLD imposes strict product liability, the AILD introduces procedural presumptions facilitating fault-based claims, and the GDPR shapes duties regarding patient data. This multi-layered framework not only ensures patient protection and innovation but also generates clear points: regulatory, professional, and product thresholds, at which the conduct of healthcare professionals using AI may trigger liability. These thresholds form the foundation for the detailed analysis developed in the following section.

2.2. Thresholds of liability for healthcare professionals under the EU AI legal framework

2.2.1. The regulatory threshold under the AI Act

The AI Act established a dedicated legal regime for AI systems placed on the Union market, with a particular focus on high-risk systems. By defining high-risk AI as systems whose malfunction may cause serious harm to health, safety, or fundamental rights, the Act automatically captures clinical decision support systems, diagnostic algorithms, and

[9] Recital 15 from the European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final, September 28, 2022.

AI-enabled medical devices. In doing so, it sets a preventive threshold of diligence for providers, deployers, and users of such systems (Aboy, Minssen, Vayena 2024, 2). But, not all AI systems used in healthcare are considered high-risk. In healthcare, high-risk AI systems include AI medical devices used for diagnosis, prevention, monitoring, prediction, prognosis, treatment, or alleviation of disease, injury, or disability, as well as certain AI applications such as evaluating emergency calls or dispatching first responders. These devices must comply with strict safety, quality, and human oversight requirements, and undergo a third-party conformity assessment under the EU Medical Devices Regulation. The AI Act adds an extra regulatory layer specifically for AI-enabled medical devices, supplementing existing MDR rules (Kolfschooten, van Oirschot 2024, 2).

At the center of this framework are a series of core obligations that directly shape liability exposure, including risk management and conformity, human oversight, transparency and information duties, and registration and monitoring. These obligations, together, delineate the regulatory threshold and directly shape the contours of liability for healthcare professionals. Before involving in the explanatory text on these obligations we would like to clarify that in the context of the AI Act, the notions of *user* and *deployer* are particularly relevant for healthcare, where we interpret them respectively as referring to individual healthcare professionals and healthcare institutions. As the literature notes, the "user" is not defined by technical expertise or development activity but by the factual role of employing an AI system within a concrete decision-making process, thereby assuming responsibility for its application in practice (Jacobs, Judith 2022). This distinction is crucial for the analysis of the AI Act (especially specific articles such as Arts 13 and 23), since the allocation of transparency and information duties depends on whether the obligations fall on professionals in their role as users or on institutions as deployers.

2.2.1.1. Risk management and conformity

Articles 9–11 require providers of high-risk AI systems to implement a risk management system, ensure data governance, produce technical documentation, and undergo conformity assessment prior to market placement[10]. These obligations form the regulatory baseline for lawful deployment. Failure to comply not only exposes providers to administrative sanctions (Art. 71) but also triggers consequences under the rPLD: non-conforming systems may be classified as defective products, with strict liability for resulting harm. Once the AILD is adopted, failure to meet conformity obligations will also generate presumptions of causation in civil claims. Thus, the conformity regime connects directly to liability attribution. These are not obligations imposed directly on healthcare professionals, but they form part of the regulatory threshold that frames the environment in which professionals operate because of the indirect and direct impact of these obligations. If a healthcare professional uses an AI system that has not undergone proper conformity assessment, liability may shift toward the manufacturer/provider under rPLD, which

[10] For high-risk systems, the Act prescribes obligations such as risk management, technical documentation, transparency, post-market monitoring, and third-party conformity assessment to ensure that natural persons can effectively oversee their functioning. It also introduces regulatory sandboxes and real-world testing mechanisms to support responsible development and deployment at national level. At present, no binding national policies supplement these requirements (Schmidt et al. 2024, 2).

creates the indirect impact of the act. The direct impact derives from the presumptions of causation provided with the AILD proposal, that can affect professional liability if a healthcare professional relies on a non-conforming AI system.

2.2.1.2. Human oversight

Article 14 requires that high-risk AI systems be designed for effective human oversight, including the ability to intervene or discontinue operation. Under this article liability for oversight falls on providers and users of high-risk AI. Users become liable when they fail to implement the human oversight measures specified by the provider, even though they retain discretion in how to organise their own resources and activities. In other words, liability arises not from the choice of method, but from a failure to ensure that the provider's oversight requirements are effectively fulfilled (Enqvist 2023, 524). In addition, Art. 14 introduces the obligation for providers to ensure that overseers will be able to duly monitor its operation, and that providers should equip the system in such a way that overseers are able to intervene on the system's operation or interrupt the system through a 'stop' button or a similar procedure (Enqvist 2023, 526). Although the AI Act itself does not impose direct negligence liability on healthcare professionals, neglect of oversight mechanisms is likely to be treated as professional fault under national malpractice regimes. The oversight clause effectively extends the duty of care, reinforcing that healthcare professionals remain the ultimate decision-makers in patient care (Kaltenbrunner 2025). In this context, Art. 14 is interpreted as requiring healthcare professionals to recognize when uncertainty exceeds an acceptable threshold and to actively intervene, through second opinions, further testing, or rejecting AI recommendations, rather than relying passively on the system (Onitiu 2022). Beyond mere compliance, the duty of human oversight can be understood as a moral imperative to engage in 'shared responsibilities,' a process where clinicians, institutions, and developers voluntarily assume answerability for the inherent 'responsibility gaps' created by black-box AI, even in the absence of strict blameworthiness (Lang, Nyholm, Blumenthal-Barby 2023, 11).

2.2.1.3. Transparency and information duties

Articles 13 and 23 mandate that providers furnish users with clear and accessible information about system capabilities, limitations, accuracy, and intended use (Aboy, Minssen, Vayena 2024). When considering AI systems in healthcare, transparency can be understood as operating on three interconnected layers. The external layer involves transparency from healthcare professionals toward patients, the internal layer refers to transparency from AI providers toward healthcare professionals, and the insider layer reflects transparency that AI providers have toward themselves. These layers mutually influence one another: patients' transparency needs shape healthcare professionals' expectations from AI providers, while the extent to which AI providers understand their own systems limits how much they can explain to healthcare professionals. Such limitations arise from the black-box nature of AI, where the internal functioning of algorithms and the precise transformation of inputs into outputs are often not fully comprehensible (Kiseleva, Kotzinos, Hert 2022, 16). Under the transparency and information duties of Arts 13 and 23 AI Act, the threshold of liability for healthcare professionals lies in their obligation to actively

interpret and verify AI outputs, and to communicate them in a patient-comprehensible manner. Failure to exercise this diligence in ensuring oversight and informed consent establishes their liability (Kiseleva, Kotzinos, Hert 2022, 11–13).

2.2.1.4. Registration and monitoring

Articles 51 and 61–67 require all high-risk AI systems to be registered in the EU-wide database and subject to continuous post-market monitoring. Deployers, including hospitals and healthcare professionals, are obliged to maintain logs, report incidents, and suspend use where risks are detected. Non-compliance exposes institutions to fines and may serve as evidence of breach of statutory duty in malpractice claims.

2.2.2. The regulatory threshold under GDPR

The General Data Protection Regulation (GDPR) sets out a regulatory threshold that directly informs liability in the healthcare sector, where personal data processing is inseparable from professional practice. For healthcare professionals, compliance with preventive obligations is not merely administrative but forms part of their professional duty of care. In this sense, the GDPR transforms data protection failures into potential sources of medical liability, since breaches may be framed as violations of both regulatory and professional standards (Hert, Papakonstantinou 2016).

At a doctrinal level, four categories of preventive obligations stand out as central to establishing liability thresholds for healthcare professionals.

2.2.2.1. Oversight duties

In the healthcare context, oversight of medical AI encompasses both patient-facing and regulatory dimensions. Professionals must ensure that patients receive sufficient information to give informed consent and meaningfully participate in shared decision-making, reflecting fundamental rights and the GDPR's safeguards (Schneeberger, Stoger, Holzinger 2020, 222). On the other hand, under Art. 24 GDPR, controllers, including healthcare institutions and individual healthcare professionals, must implement technical and organisational measures and be able to demonstrate compliance. The accountability principle in Art. 5 (2) reinforces this requirement by obliging professionals to prove adherence when challenged. Supervisory authorities, empowered by Arts 51–58, may demand such demonstrations, making oversight continuous. In healthcare, inadequate oversight can be regarded as both regulatory non-compliance and a breach of professional responsibility, thereby influencing liability (Voigt, Bussche 2017).

2.2.2.2. Conformity assessment of high-risk processing

Article 35 requires Data Protection Impact Assessments (DPIAs in the further text) when processing operations involve high risks, such as large-scale use of health data or deployment of AI-based diagnostic systems. Where risks cannot be mitigated, consultation with supervisory authorities under Art. 36 is mandatory. For healthcare professionals, DPIAs reflect the duty to anticipate risks before treatment or innovation is introduced. As

studies show, DPIAs in medical research and hospital settings highlight risk identification and compliance gaps, ensuring that liability is tied not only to outcomes but also to preventive assessment (Compagnucci, Dahi, Davis 2023). This anticipatory duty mirrors the medical standard of care, where risk assessment and prevention are central to liability determination (Wachter, Mittelstadt 2019).

2.2.2.3. Documentation and demonstration of compliance

Articles 30 and 33–34 impose record-keeping and breach notification duties. For healthcare professionals, this translates into maintaining detailed logs of medical data processing and reporting breaches within the 72-hour window. The legal importance of documentation goes beyond transparency: it functions as evidence of due diligence in case of disputes over medical liability (Wachter, Mittelstadt 2019). Failure to produce adequate records may be treated as negligence per se. The GDPR thereby shifts liability towards structural compliance, meaning healthcare professionals may be held accountable for failing to produce records even in the absence of demonstrable patient harm (Voigt, Bussche 2017).

2.2.2.4. Data governance and preventive design

Article 25 establishes data protection by design and by default, requiring healthcare systems to integrate privacy into their technologies and workflows. Article 32 further requires security measures proportional to risks, such as encryption or pseudonymization of health records. These governance obligations directly affect liability standards, since professionals are expected to ensure that clinical practices and IT systems comply with these requirements. Governance failures may thus be treated analogously to medical malpractice, as they reflect preventable harm through omission. In healthcare, weak governance or security lapses, such as inadequate system resilience or unprotected storage of medical files, may amount to breaches of both regulatory obligations and professional standards of care (Fuster 2014).

Taken together, these obligations define the regulatory threshold that healthcare professionals must meet. Unlike traditional liability frameworks that focus on harm, GDPR liability attaches to failures in preventive duties themselves. In medical settings, this means a professional can incur liability for failing to conduct a DPIA, maintain documentation, or implement governance measures, even if no patient has yet suffered material damage (Hert, Papakonstantinou 2016; Wachter, Mittelstadt 2019).

2.2.3. The regulatory threshold under the MDR

The MDR establishes a comprehensive framework for ensuring the safety, effectiveness, and compliance of medical devices. While much of the Regulation is directed at manufacturers and notified bodies, healthcare professionals play a critical role in ensuring safe application, vigilance, and conformity of devices in practice (Schmidt et al. 2024, 4). For them, the MDR sets a regulatory threshold of preventive obligations which intersect with professional liability: non-compliance may expose healthcare professionals to both regulatory sanctions and civil claims where harm arises.

The obligations for healthcare professionals under the MDR can be systematized into four main categories.

2.2.3.1. Oversight and vigilance obligations

Articles 87–90 require healthcare professionals to report serious incidents and device malfunctions to the manufacturer and competent authorities. Vigilance systems depend on the active involvement of healthcare professionals, who are often the first to detect device-related risks in clinical practice. A failure to fulfil this duty not only undermines regulatory objectives but may also be construed as negligence in professional liability contexts, as it breaches the duty to protect patient safety.

2.2.3.2. Conformity and proper use

Article 5 stipulates that devices may only be placed and used if they conform with the Regulation and bear CE marking. Healthcare professionals are expected to verify the conformity status of devices and ensure their use only for intended medical purposes. Using uncertified, expired, or improperly maintained devices constitutes a breach of the conformity threshold and may amount to negligent practice. This preventive obligation positions healthcare professionals as gatekeepers, ensuring that only compliant devices are integrated into treatment.

2.2.3.3. Documentation and traceability

The MDR introduces obligations of traceability through the Unique Device Identification (UDI) system (Arts 27 and 25(2)) and requires healthcare institutions to retain and make available device identifiers. For healthcare professionals, this entails documenting device use in patient records and ensuring that devices can be traced in case of recalls or safety issues. From a liability perspective, proper documentation serves as evidence of compliance, while inadequate records may give rise to presumptions of negligence or fault.

2.2.3.4. Governance, training, and safe use

Annex I (General Safety and Performance Requirements) and Recital 48 emphasize that medical devices must be used in accordance with instructions for use, and healthcare professionals must be adequately trained. The MDR thus embeds obligations of competence and safe integration into workflows. Professional liability arises where healthcare professionals disregard usage requirements, misuse devices, or fail to maintain necessary training, as these lapses represent breaches of both regulatory duties and professional standards of care.

Taken together, these obligations define a regulatory threshold for liability in healthcare practice under the MDR. Unlike traditional fault-based liability, which often depends on harm, the MDR aligns liability with preventive compliance: professionals may be held accountable for failing to meet oversight, conformity, documentation, or governance duties even before harm materialises. This doctrinal shift illustrates how the MDR transforms preventive obligations into benchmarks of professional responsibility in medical practice.

2.2.4. The professional threshold

The professional liability threshold for healthcare professionals in AI-related cases unfolds on two dimensions. At the national level, malpractice regimes continue to define the substantive standard of care, which differs across Member States depending on how medical negligence is regulated. At the EU level, the Proposal AILD does not harmonize these duties but instead overlays procedural mechanisms. This section examines only the EU proposal, focusing on how the AILD modifies litigation dynamics without displacing national standards of medical care, as explained in the methodology section. It is important to stress that the AILD has not yet been adopted, and therefore currently represents a *proposed harmonisation regime*. Its provisions are designed to complement the AI Act and the rPLD, while interacting with national tort and malpractice laws rather than replacing them. Recital 15 from the proposed AILD clarifies that the AILD is limited to situations where harm arises from the output (or failure to produce output) of an AI system attributable to the fault of a human actor, such as a provider or user under the AI Act. Conversely, where AI merely informs a human decision and the harm can be traced to that decision, traditional liability rules apply, as the involvement of AI does not complicate the causal chain (Clavijo 2024, 5).

The proposed AILD does not create new duties of care for healthcare professionals *ex lege* but modifies how breaches of existing duties may be established in disputes involving AI systems. These obligations can be systematized into four main categories.

2.2.4.1. Obligations of disclosure and access to evidence

Article 3 allows courts to order disclosure of evidence by providers or users of high-risk AI systems. For healthcare professionals as "users" or "deployers," this creates an indirect obligation to maintain adequate records of how AI was used in clinical decision-making. Academic commentary highlights that AILD strengthens the evidentiary position of patients by requiring providers and deployers of high-risk AI systems to disclose relevant information, with failure to comply creating a presumption of non-compliance before national courts. For healthcare professionals, this means that liability may be triggered not only by inadequate oversight of AI outputs but also when institutions or individuals obstruct or fail to facilitate disclosure of evidence needed for patients to substantiate claims (Li, Schütte 2024, 148). While the AILD's procedural mechanisms aim to lower evidentiary barriers, scholarly critique cautions that it may simply shift the claimant's burden from proving fault to accessing and interpreting complex technical evidence, potentially creating a new 'burden of evidence' and failing to address the foundational 'information gap' where victims are unaware they have been harmed by an AI system in the first place (Ziosi et al. 2023, 3, 4).

2.2.4.2. Obligations tied to presumptions of causality

Article 4 introduces a rebuttable presumption that non-compliance with AI Act obligations (such as human oversight or data governance) has caused the damage if it is reasonably likely to have influenced the outcome. This presumption applies to both providers and users, meaning healthcare professionals may face a reversed burden of proof in malpractice

claims when AI involvement is established. In other words, the presumption of a causal link introduced by the AILD functions as a threshold for liability in a manner that once a claimant shows fault and damage, courts may presume causation unless the defendant rebuts it. For healthcare professionals, this presumption could ease the evidentiary burden when harm arises from AI-assisted care, provided that the professional's fault is demonstrated (e. g., failure to comply with duties of care directly intended to prevent harm). However, the presumption is narrowly applied and limited to high-risk AI, specific duties, and cases where proving causation would otherwise be "excessively difficult", which may restrict its practical relevance. Additionally, the burden on professionals remains significant because proving compliance or rebutting causation requires demonstrating accessible evidence and material non-interference with the AI, highlighting the delicate balance between automated decision-making and professional accountability. Overall, the presumption serves as a conditional threshold, signaling that liability arises only when fault and resultant harm align under specific circumstances (Diega, Bezerra 2024). This procedural nature of the AILD is particularly significant given that, as comparative analysis shows, the primary challenge for fault-based liability in medical AI is not the substantive standard of care itself, but the severe evidentiary burdens placed on the patient due to the 'black-box effect' (Maroudas 2024, 162). However, the procedural relief offered by the AILD must be viewed in light of critiques that it privileges transparency of high-risk systems over a victim's knowledge of harm, and may not fully overcome the 'black-box' nature of AI if claimants lack the technical literacy to understand the disclosed evidence (Ziosi et al. 2023, 4, 7).

2.2.4.3. Documentation and diligence obligations

While the AILD does not directly legislate new documentation standards, it builds upon the AI Act's transparency (Art. 13) and human oversight (Art. 14) requirements. Healthcare professionals like software engineers, must ensure that AI-assisted decisions are properly documented, aligned with regulatory standards, and verifiable. The emphasis on structured methodologies, checklists, and automated compliance tools suggests that healthcare professionals could similarly adopt systematic documentation practices, for example, recording whether AI outputs were verified, overridden, or integrated into patient care. This has a direct impact on liability, because failing to maintain proper records may strengthen presumptions of fault under the AILD (Sovrano et al. 2025).

2.2.4.4. Interaction with high-risk classification

By explicitly linking liability presumptions to *high-risk AI systems*, the Directive effectively extends professional duties of care in contexts such as diagnostics, treatment planning, and predictive analytics. Here, healthcare professionals must not only rely on certified tools but must also ensure that their clinical decisions reflect the oversight mechanisms mandated by the AI Act. Scholars have noted that this integration of AI into malpractice law creates a hybrid threshold, combining professional judgment with statutory oversight requirements. The AILD excludes cases where harm results from a human act informed by AI advice, as causality can be traced to the human actor, yet this interacts with the AI Act's high-risk classification, which mandates that such systems be designed for effective human oversight, potentially limiting the directive's applicability (Clavijo 2024, 3).

2.2.5. The product threshold

The rPLD establishes the definitive product threshold of liability by focusing compensation on risk allocation rather than fault (Buiten 2024). This framework explicitly complements, yet operates independently from, the professional negligence rules governing medical malpractice. The central function of the PLD is to manage the residual safety risks not entirely eliminated by the preventive *ex ante* regulations of the AI Act and the MDR. For the healthcare professionals, liability depends entirely on the nature of their interaction with the AI tool: compliant use is judged against the professional standard of care (the Professional Threshold), whereas unauthorized modification or misuse that impacts the device's safety baseline triggers the strict liability of the Product Threshold. This divergence ensures that while the opacity of AI does not prevent patient compensation, responsibility is assigned based on control, particularly where professional choices transform a certified product's intrinsic safety.

The types of interaction between doctors and AI systems can be categorized into three main frameworks: reliance, oversight, and collaborative decision-making. Doctors may rely on AI systems for decision-making, especially in diagnostic contexts where AI analyzes medical images or data. This reliance is complicated by the risk of "automation bias", where healthcare professionals may overlook critical information outside the AI's suggestions due to undue trust in the AI's recommendations, leading to potential misdiagnoses or errors (Verdicchio, Perin 2022). When it comes to oversight of AI recommendations, healthcare professionals maintain a critical eye on AI outputs, assessing their validity before taking action. This requires doctors to be aware of the AI's limitations and to conduct independent evaluations of the AI's suggestions, thus ensuring that patient care decisions are based on a blend of AI analysis and human judgment. The collaborative decision-making emphasizes a partnership between doctors and AI, where both contribute to the decision-making process. Doctors use AI as a supplementary tool that enhances their clinical expertise rather than replacing it, fostering an environment where AI assists in providing a comprehensive view of patient information while healthcare professionals remain accountable for the final decisions (Verdicchio, Perin 2022, 23).

For this paper, we have categorized the obligations under the rPLD into three key thresholds: 1) the inclusion of digital products and software, 2) the allocation of liability through substantial modification, and 3) procedural relief and evidentiary burdens, each highlighting different aspects of how liability may arise for healthcare professionals using AI-enabled medical technologies.

2.2.5.1. Inclusion of digital products and software

The PLD fundamentally expands the definition of "product" to encompass software, operating systems, applications, and standalone AI systems (Montagnani, Najjar, Davola 2024, 12; Arcila 2024, 9). This inclusion is crucial for highly regulated sectors like healthcare, ensuring that strict liability applies to defective digital components, whether embedded in a medical device or functioning as stand-alone software (Clavijo 2024, 3). By recognizing software as a product, the Directive ensures that harms arising from defective medical AI tools, whether embedded in devices or operating as stand-alone software, can give rise to liability regardless of the healthcare professional's own diligence (Buiten 2024,

251). This framework holds the manufacturer or other economic operator strictly liable for product defects that cause harm, regardless of whether the defect could have been known at the time the product was placed on the market (Arcila 2024, 6).

The doctrinal challenge arises where a machine-learning system generates erroneous predictions that compromise patient health. Unlike printed information or static software outputs, which the Court of Justice has previously excluded from product liability (Case C-65/20, *VI v. KRONE*)[11], AI systems are dynamic entities designed to perform a specific medical function. Their predictive outputs are not ancillary information but constitute the core functionality of the system itself. Accordingly, an inaccurate medical assessment produced by such a system may qualify as a defect because it undermines the product's intended purpose — safe and reliable medical decision support (Clavijo 2024). This interpretation is significant for healthcare professionals. If predictive AI systems are themselves classed as defective products, liability claims can extend beyond healthcare professionals and reach the broader chain of economic operators involved in development and distribution, including manufacturers, importers, and authorised representatives. For healthcare professionals this reduces direct liability exposure for defects intrinsic to the AI system, but it also raises the threshold of diligence: professionals must ensure they are using certified and compliant AI tools, as reliance on non-compliant systems could shift liability back onto them through negligence or substantial modification.

2.2.5.2. Allocation of liability through substantial modification

One of the most significant innovations lies in the Directive's *expanded subjective scope*. Liability is no longer confined to the original producer but now follows a layered model that encompasses a broader range of economic operators. This includes authorised representatives, importers, fulfilment service providers, and, under certain conditions, distributors. In addition, natural or legal persons who substantially modify a product outside the manufacturer's control and subsequently make it available on the market or put it into service are treated as manufacturers for liability purposes. This layered approach ensures that compensation remains accessible even if the original producer cannot be identified or is not established in the EU (Montagnani, Najjar, Davola 2024, 11). For healthcare professionals, this provision is particularly relevant: by altering the functioning of AI-enabled medical devices, they may unintentionally move from the position of user to that of producer, thereby becoming subject to strict liability. This is essentially the mechanism by which a healthcare professional crosses the Product Threshold and it is formalized through the expansion of the subjective scope of liability, particularly regarding modification. The PLD stipulates that any natural or legal person who substantially modifies a product outside the original manufacturer's control and subsequently places it on the market or puts it into service is treated as the producer for liability purposes (Arcila 2024, 9). This rule is decisive in healthcare. Actions by a healthcare professional, such as overriding safety parameters, integrating unauthorized software components, or utilizing a certified AI device outside its intended use, may constitute a substantial modification. These actions transition the healthcare professional's legal status from a user/deployer—

[11] Court of Justice of the European Union (2021). *VI v. KRONE, Case C-65/20*. ECLI:EU:C:2021:471, Judgment of June 10, 2021. Accessed December 24, 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62020CJ0065.

subject to the professional duty of care — to a *de facto modifier* or manufacturer, thereby incurring strict liability for resulting defects. This structural shift ensures that risk is allocated to the party exercising the highest degree of control over the final safety configuration of the product (Buiten 2024). Moreover, the interpretation of key concepts such as "modifications," "defect," and "substantial modification" remains subject to uncertainty. For instance, whether self-learning capabilities of AI software constitute a modification will likely depend on how courts interpret the scope of a "manufacturer's control." These ambiguities are expected to be gradually clarified through decisions at both national and European levels. Courts will need to develop a technical understanding of AI systems, their functioning, and associated risks to appropriately apply liability standards. This includes assessing whether a professional's behavior meets the standard of care, which varies according to the current state of technology, sector-specific safety standards, and established scientific and technical frameworks. This foundational understanding is particularly relevant in highly regulated sectors such as healthcare, where AI-enabled tools are increasingly integral to medical decision-making (Montagnani, Najjar, Davola 2024, 13).

2.2.5.3. Procedural relief and evidentiary burdens

To overcome the inherent informational asymmetry and technical opacity ("black-box" nature) of AI systems, the Directive also introduces *rebuttable presumptions of defectiveness and causation* in situations where proving technical fault is excessively difficult. These presumptions alleviate the evidentiary burden on injured patients while simultaneously increasing the pressure on manufacturers and users to demonstrate compliance with safe use protocols (Arcila 2024, 9). This procedural innovation significantly alleviates the evidentiary burden on the injured patient, making it easier to prove a claim against a manufacturer or a de facto producer (Montagnani, Najjar, Davola 2024, 13). Simultaneously, this measure increases the regulatory pressure on manufacturers and deployers (including healthcare professionals performing substantial modifications) to ensure robust compliance, logging, and documentation of the system's design and use to rebut these legal presumptions in court.

3. Conclusions

This paper has demonstrated that the liability of healthcare professionals using AI is best understood through a threshold typology that distinguishes regulatory, professional, and product dimensions. This framework is essential to navigate the complex accountability challenges, including the "black-box problem" and resulting responsibility gaps, posed by the integration of AI into clinical care. The developed typology does not merely describe legal sources but identifies the critical junctures at which professional conduct shifts from compliance to liability, offering a structured lens for analyzing accountability in medical AI.

To systematize this complex framework, the analysis has introduced the concept of core duties in conclusion. These represent the obligations that consistently appear across the thresholds as baseline standards of care. The term *core duties* is adopted because it captures the dual function of these obligations: they operate preventively, by shaping lawful deployment and professional practice, while also serving as liability benchmarks when

Table 2. **Core duties across liability thresholds**

Threshold	Legal Source(s)	Core Duties
Regulatory Threshold	Artificial Intelligence Act (Regulation (EU) 2024/1689); Medical Device Regulation (Regulation (EU) 2017/745); General Data Protection Regulation (Regulation (EU) 2016/679)	Risk management, conformity assessment, transparency, data governance, human oversight
Professional Threshold	National tort/malpractice law; AI Liability Directive Proposal (COM(2022) 496 final)	Duty of care, diligence in oversight, proper documentation, patient information and informed consent
Product Threshold	Product Liability Directive (Revised) (Directive (EU) 2024/1799)	Safe use of certified devices, no substantial modification, no off-label use or misuse

breaches occur. The accompanying table (see Table 2) synthesizes the thresholds, their legal sources, and the corresponding core duties that define this new liability landscape.

The regulatory threshold is defined by preventive duties under the AI Act, the MDR, and the GDPR. These instruments do not primarily impose fault liability, but rather establish an *ex ante* compliance environment through risk management, conformity assessment, transparency, data protection, and vigilance obligations. Breaches of these obligations may later inform liability by serving as benchmarks for standard of care or as triggers for product defect classification.

The professional threshold is shaped by national malpractice law, but its contours are increasingly harmonised procedurally through the proposed AILD. Here, liability arises from breaches of the medical duty of care in contexts where AI is integrated into clinical decision-making. The AILD's presumptions of causality and disclosure obligations lower evidentiary barriers for patients and thereby reinforce the oversight role of healthcare professionals. This threshold reflects the hybridisation of professional responsibility with statutory oversight requirements, creating a shared accountability regime.

The product threshold, consolidated in the rPLD, provides strict liability for defective AI-enabled products. While primarily targeting manufacturers and other economic operators, this framework directly affects healthcare professionals when they substantially modify certified AI systems or use them outside their intended purposes. In such cases, the professional crosses into the role of de facto producer, thereby assuming strict liability for defects.

Taken together, these thresholds illustrate that liability in medical AI is not located in a single legal instrument, but emerges from the interaction of five EU acts. The AI Act and MDR establish the preventive safety and conformity regime, the GDPR embeds data protection as a professional duty, the rPLD secures compensation through strict product liability, and the AILD adapts fault-based claims to the opacity of AI. Their intersection creates a layered system in which healthcare professionals are simultaneously subject to regulatory compliance standards, professional duties of care, and product-related responsibilities, depending on the nature of their interaction with AI systems.

The added value of the threshold typology is its capacity to translate this complex legal architecture into an operational framework. For lawyers, it clarifies the doctrinal

bases of liability attribution across instruments; for healthcare professionals, it identifies the practical points at which oversight lapses, misuse, or modification may expose them to legal consequences. The typology also reveals that liability is both distributed and conditional: distributed across multiple legal layers, and conditional upon the role a professional assumes in practice—user, overseer, or modifier.

Ultimately, the analysis shows that the EU framework does not merely impose liability after harm, but actively embeds liability into preventive structures of oversight, transparency, and conformity. This signals a shift from reactive compensation to proactive governance of medical AI. In this sense, the threshold typology not only explains the current state of law but also offers a doctrinal map for future adjudication and legislative development in the field of medical AI liability. Future research should expand the analysis by integrating judicial practice and empirical evidence to strengthen the understanding of liability thresholds in practice.

References

Aboy, M., T. Minssen, E. Vayena. 2024. "Navigating the EU AI Act: Implications for regulated digital medical products". *NPJ Digital Medicine* 6–7 (1): 237. https://doi.org/10.1038/s41746-024-01232-3

Ampovska, M. 2024. "European Union civil liability frameworks in the age of artificial intelligence: Assessing current regimes and future prospects". *Vestnik of Saint Petersburg University. Law* 2: 466–482.

Arcila, B. B. 2024. "AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight?" *Computer Law & Security Review* 54: 1–17.

Bagave, P., M. Westberg, M. Janssen, A. Y. Ding. 2025. "Accountability framework for healthcare AI systems: Towards joint accountability in decision making". *Frontiers in Artificial Intelligence* 8: 1–15.

Ballell, T. R. 2023. "'The revision of the product liability directive: A key piece in the artificial intelligence liability puzzle". *ERA Forum* 24: 247–259. https://doi.org/10.1007/s12027-023-00751-y

Buiten, M. C. 2024. "Product liability for defective AI". *European Journal of Law and Economics* 57: 239–273. https://doi.org/10.1007/s10657-024-09794-z

Clavijo, S. C. 2024. "AI assessment tools for decision-making on telemedicine: Liability in case of mistakes". *Discover Artificial Intelligence* 4: 1–6.

Compagnucci, M. C., A. Dahi, P. E. Davis. 2023. "Conducting a Data Protection Impact Assessment in Health Science: A Comprehensive Guide". *SSRN* December 8: 1–23. https://dx.doi.org/10.2139/ssrn.4651993

Diega, G. N., L. C. T. Bezerra. 2024. "Can there be responsible AI without AI liability? Incentivizing generative AI safety through ex-post tort liability under the EU AI liability directive". *International Journal of Law and Information Technology* 32: 1–21.

Enqvist, L. 2023. "'Human oversight' in the EU artificial intelligence act: What, when and by whom?" *Law, Innovation and Technology* 15 (2): 508–535. https://doi.org/10.1080/17579961.2023.2245683

Fuster, G. G. 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Cham, Springer. https://doi.org/10.1007/978-3-319-05023-2

Hacker, P. 2023. "The European AI liability directives — Critique of a half-hearted approach and lessons for the future". *Computer Law & Security Review* 51: 1–42.

Hert, P. D., V. Papakonstantinou. 2016. "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" *Computer Law & Security Review* 32 (2): 179–194.

Jacobs, M., S. Judith. 2022. "Assigning obligations in AI regulation: A discussion of two frameworks proposed by the European Commission". *Digital Society* 6: 1–23.

Kaltenbrunner, S. 2025. "Human in control: Shared decision-making with clinical decision-support systems under the Artificial Intelligence Act". *SSRN* January 17. Accessed September 20, 2024. https://ssrn.com/abstract=5093935.

Kiseleva, A., D. Kotzinos, P. De Hert. 2022. "Transparency of AI in healthcare as a multilayered system of accountabilities: Between legal requirements and technical limitations". *Frontiers in Artificial Intelligence* 5: 1–21. https://doi.org/10.3389/frai.2022.879603

Kolfschooten, H. V., J. van Oirschot. 2024. "The EU Artificial Intelligence Act (2024): Implications for healthcare". *Health Policy* 149: 1–9. https://doi.org/10.1016/j.healthpol.2024.105152
Lang, B. H., S. Nyholm, J. Blumenthal-Barby. 2023. "Responsibility gaps and black box healthcare AI: Shared responsibilization as a solution". *Digital Society* 52: 1–17. https://doi.org/10.1007/s44206-023-00073-z
Li, S., B. Schütte. 2024. "The proposed EU Artificial Intelligence Liability Directive — Does/will its content reflect its ambition?" *Technology and Regulation*: 143–151. https://doi.org/10.26116/techreg.2024.014
Maroudas, V. P. 2024. "Fault-based liability for medical malpractice in the age of artificial intelligence: A comparative analysis of German and Greek medical liability law in view of the challenges posed by AI systems". *Review of European and Comparative Law* 51 (2): 135–169.
Montagnani, M. L., M.-C. Najjar, A. Davola. 2024. "The EU regulatory approach(es) to AI liability, and its application to the financial services market". *Computer Law & Security Review: The International Journal of Technology Law and Practice* 53: 1–19.
Onitiu, D. 2022. "The limits of explainability & human oversight in the EU Commission's proposal for the Regulation on AI — a critical approach focusing on medical diagnostic systems". *Information & Communications Technology Law* 32 (2): 170–188. https://doi.org/10.1080/13600834.2022.2116354
Schmidt, J., N. Schutte, S. Buttigieg, D. Novillo-Ortiz, E. Sutherland, M. Anderson, B. de Witte, M. Peolsson, B. Unim, M. Pavlova, A. D. Stern, E. Mossialos, R. van Kessel. 2024. "Mapping the regulatory landscape for artificial intelligence in health within the European Union". *NPJ Digitale Medicine* 7 (1): 1–9.
Schneeberger, D., K. Stoger, A. Holzinger. 2020. "The European legal framework for medical AI". *Machine Learning and Knowledge Extraction*, 209–226. https://dl.acm.org/doi/10.1007/978-3-030-57321-8_12
Smith, H. 2021. "Clinical AI: Opacity, accountability, responsibility and liability". *AI & Society* 36: 535–545. https://doi.org/10.1007/s00146-020-01019-6
Sovrano, F., E. Hine, S. Anzolut, B. Alberto. 2025. "Simplifying software compliance: AI technologies in drafting technical documentation for the AI Act". *Empirical Software Engineering Volume* 91: 1–36. https://doi.org/10.1007/s10664-025-10645-x
Verdicchio, M., A. Perin. 2022. "When doctors and AI interact: On human responsibility for artificial risks". *Philosophy & Technology* 11: 1–28.
Voigt, P., A. von dem Bussche. 2017. *The EU General Data Protection Regulation (GDPR): A Practical Guide.* Cham, Springer.
Wachter, S., B. Mittelstadt. 2019. "A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI". *Columbia Business Law Review* 2: 494–620.
Ziosi, M., J. Mökander, C. Novelli, F. Casolari, M. Taddeo, L. Floridi. 2023. "The EU AI Liability Directive (AILD): Bridging information gaps". *European Journal of Law and Technology* 14 (3): 1–10.

Received: October 4, 2025
Accepted: October 30, 2025

Author's information:

Marija Ampovska — Full Professor; https://orcid.org/0000-0002-9147-5890,
marija.ampovska@ugd.edu.mk

Пределы свободы воли в медицинском искусственном интеллекте: система ответственности медицинских работников в соответствии с законодательством Европейского союза

М. Амповска

Университет Гоце Делчева,
Республика Северная Македония, 2000, Штип, ул. Крште Мисирков, 201

Для цитирования: Ampovska, M. 2026. "Thresholds of agency in medical artificial intelligence: A liability framework for healthcare professionals under European Union law". *Вестник Санкт-Петербургского университета. Право* 1: 109–127. EDN LUWFEI

Быстрая интеграция сложного искусственного интеллекта (ИИ) в клиническую практику представляет собой смену парадигмы здравоохранения, бросающую вызов традиционным представлениям об ответственности врачей и требующую нового нормативного правового регулирования. В статье предлагается «пороговая типология» для систематического анализа ответственности медицинских работников в рамках сложной и многоуровневой нормативно-правовой базы Европейского союза. По мнению автора, вопрос ответственности зависит от того, какой из трех порогов свободы воли переступает врач в пользу ИИ. Первым порогом является нормативный, он установлен превентивными и предварительными обязательствами Закона об искусственном интеллекте (Artificial Intelligence Act, AI Act), Общим регламентом по защите данных (General Data Protection Regulation, GDPR) и Регламентом по медицинскому оборудованию (Medical Device Regulation, MDR). Этот порог фокусируется на соблюдении обязанностей по управлению рисками, по надзору, управлению данными и бдительности, когда нарушения могут повлиять на последующую ответственность. Затем проверяется профессиональный порог, определенный в соответствии с основанными на вине стандартами национального законодательства о недобросовестной практике, которые процедурно адаптированы предлагаемой Директивой об ответственности за ИИ (AI Liability Directive AILD) с помощью таких механизмов, как раскрытие доказательств и опровержимые презумпции причинно-следственной связи. Наконец, изучается порог использования продукта, основанный на режиме «строгой ответственности», предусмотренном пересмотренной Директивой об ответственности за качество продукции (revised Product Liability Directive, rPLD), которая актуализируется, когда медицинские работники существенно модифицируют системы искусственного интеллекта, фактически исполняя роль производителя. Благодаря тщательному анализу взаимодействия между этими пятью ключевыми инструментами ЕС — Законом об ИИ, AILD, rPLD, GDPR и MDR — в статье формулируется авторский подход, демонстрирующий, что ответственность является условной, распределенной и в значительной степени зависит от контекста, в зависимости от того, выступает ли профессионал в качестве пользователя, наблюдателя или модификатора системы ИИ. Таким образом, «пороговая типология» служит жизненно важным аналитическим инструментом, преобразующим фрагментированную правовую архитектуру в согласованную и оперативную структуру для ученых-юристов, практиков и медицинских работников, одновременно сигнализируя о более широком переходе от реактивной компенсации к активному управлению медицинским ИИ.

Ключевые слова: ответственность за искусственный интеллект в медицине, законодательство Европейского союза в области искусственного интеллекта, медицинские работники, порог ответственности, директива об ответственности за качество продукции, обязанность по уходу, строгая ответственность, виновная ответственность.

Статья поступила в редакцию 4 октября 2025 г.;
рекомендована к печати 30 октября 2025 г.

Контактная информация:

Амповска Мария — проф.; https://orcid.org/0000-0002-9147-5890,
marija.ampovska@ugd.edu.mk