European Journal of Risk Regulation (2026), 1–17
doi:10.1017/err.2026.10176

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Hospitals as AI Deployers: Organisational Failures and Direct Liability Risks

Claudia Giorgetti[1], Giuseppe Contissa[1] and Arianna Giorgetti[2]

[1]Department of Legal Studies, University of Bologna, Italy and [2]Department of Medical and Surgical Sciences, University of Bologna, Italy

Corresponding author: Claudia Giorgetti; Email: claudia.giorgetti6@unibo.it

Abstract

The present study aims to investigate the direct liability risk borne by hospitals (fault-based liability, hinging on the organisational failures of the hospital) when they deploy an AI-based medical device, with particular attention to clinical decision support systems. To do so, the article analyses the choices that hospitals make when deploying new medical devices, their sphere of control and the concrete likelihood of having to pay for damages. The study first reconstructs the lifecycle of deployment of AI systems by hospitals, through five different phases, and identifies the related organisational decisions that may generate foreseeable risks if inadequately performed and thus may lead to direct liability. The analysis then shifts to reconstructing the relevant spheres of control: it is highlighted how hospital and AI provider both contribute to the creation of the clinical environment, within which the physician exercises clinical discretion. The study further examines the concrete exposure of hospitals to direct liability on the basis of structural obstacles that claimants face and the circumstances under which recognising such liability becomes more realistic.

Keywords: liability risk; hospital; medical AI

I. Introduction

Artificial intelligence (AI) is known to create significant liability issues, particularly in regard to uncertainty in its allocation.[1] Healthcare is a sector where AI has found fertile ground only in more recent years, and as such where the issue of liability is underexplored compared to fields where automation has a longer tradition (such as aviation and self-driving cars).[2] AI technologies used in healthcare are typically developed by external providers, although healthcare facilities may also develop such systems in-house or in collaboration with technology companies. Some particularly relevant AI systems in the field are Clinical Decision Support Systems (CDSSs), which are aimed at aiding physicians

[1] A. Bertolini, *Artificial Intelligence and Civil Liability: A European Perspective* (European Parliamentary Research Service (EPRS) 2025); C. Giorgetti, A. Giorgetti and R. Boscolo-Berto, "Establishing New Boundaries for Medical Liability: The Role of AI as a Decision-Maker" (2025) 34 Advances in Clinical and Experimental Medicine 1601.

[2] G. Contissa and others, "Liability and Automation: Issues and Challenges for Socio-Technical Systems" (2013) 2 Journal of Aerospace Operations; G. Contissa, "Automation and Liability: An Analysis in the Context of Socio-Technical Systems" (2017) 11 I-LEX 17 <https://www.i-lex.it/articles/volume11/fascicolo1/contissa_automation_and_liability.pdf> (last accessed 13 May 2026).

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/err.2026.10176

in clinical decision-making tasks,[3] and most relevantly those of selecting the diagnosis and the treatment options. These decisions are some of the most crucial in terms of liability, since usually harms to patients' health can be traced back to these stages of decision-making.[4]

AI systems operate within what can be defined as complex socio-technical systems,[5] intended as systems which, in order to function, require close cooperation between three components: humans, machines and institutions.[6] In the case of AI systems in healthcare, this usually translates into healthcare professionals, AI-powered medical devices, and healthcare facilities.[7]

Usually when it comes to AI and liability, attention tends to be given to the technical side, meaning the potential liability of economic operators such as manufacturers, importers, etc. The EU's recent initiatives, in fact, focus precisely on said figures: consider the revision of the Product Liability Directive (2024/2853) and the now discarded proposal for an Artificial Intelligence Liability Directive (COM/2022/496 final). The institutional component tends, instead, to be overlooked for its potential liability risk.

Moreover, when it comes to the medical field, it is common to consider harm as something caused by individuals rather than by organisations. It is widely recognised that "to err is human,"[8] meaning, in the medical liability field, that medical errors are always going to occur. The focus, however, should not just be on individual AI providers, but rather also on organisational failures. Acknowledging organisational failures, while not an excuse for the conduct of the negligent physician, is the first step towards a better approach for preventing medical errors.[9]

From a liability standpoint, harm is usually traced back to individual actions, even though there are often latent conditions that cause or contribute to errors, including organisational factors.[10] The role of the organisation becomes all the more important in complex systems,[11] such as clinical care, and even more so AI-integrated ones.

It is thus crucial to investigate the possible liability risks borne by healthcare facilities when deploying AI-powered medical devices, and particularly those used in clinical practice, such as CDSSs. To this end, it is important to understand the role of the healthcare facility in deploying these systems, and how said role may in turn be reconnected to harm.

[3] R. T. Sutton and others, "An Overview of Clinical Decision Support Systems: Benefits, Risks, and Strategies for Success" (2020) 3 NPJ Digital Medicine 1 <https://doi.org/10.1038/s41746-020-0221-y> (last accessed 13 May 2026); M. Elhaddad and S. Hamam, "AI-Driven Clinical Decision Support Systems: An Ongoing Pursuit of Potential" (2024) 16 Cureus e57728 <https://doi.org/10.7759/cureus.57728> (last accessed 13 May 2026).

[4] S. D. Ferrara and others, "Malpractice and Medical Liability. European Guidelines on Methods of Ascertainment and Criteria of Evaluation" (2013) 127 International Journal of Legal Medicine 545.

[5] E. Trist, "The Evolution of Socio-Technical Systems: A Conceptual Framework and an Action Research Program" (Ontario Quality of Working Life Centre 1981) Occasional Paper 2.

[6] F. Lagioia and G. Contissa, "The Strange Case of Dr Watson: Liability Implications of AI Evidence-Based Decision Support Systems in Health Care" (2020) 12 European Journal of Legal Studies 245 <https://cris.unibo.it/retrieve/e1dcb335-c971-7715-e053-1705fe0a6cc9/EUI_journal_Lagioia%20%28EE%2029.06%29%20FINAL%20VERSION.pdf> (last accessed 13 May 2026).

[7] Ibid.

[8] D. H. Havens and L. Boroughs, "' To Err Is Human': A Report from the Institute of Medicine" (2000) 14 Journal of Pediatric Health Care 77.

[9] Ibid.; L. L. Leape, "Error in Medicine" (1994) 272 JAMA 1851.

[10] M. Duffourc, "Liability for Negligent Healthcare Clinical Risk Management in the United States and Germany" (PhD thesis, Universität Passau 2023).

[11] Ibid.; A. Pauli-Wagner and C. Thomeczek, "Risikomanagement und CIRS als Gegenstand der Krankenhaushaftung – eine Betrachtung von CIRS im Kontext der Patientensicherheit" in C. Katzenmeier (ed), *Festschrift für Dieter Hart: Medizin - Recht - Wissenschaft* (Springer 2020).

https://doi.org/10.1017/err.2026.10176

Healthcare facilities can be considered liable according to two different liability regimes[12]:

- direct liability: fault-based liability, hinging on organisational failures.
- indirect liability: vicarious liability for the conduct of the physician.

The focus of this study is on direct liability, as it concerns the choices of the organisation. The study proceeds with the assumption that the healthcare facility, from now on shortened as hospital, is a third party to the AI, who has not contributed in any manner to the development of the system, and does not provide any substantial modifications that would lead to the applicability of the revised Product Liability Directive (Article 8(2) PLD), for the sake of simplicity.

It is fundamental to consider that AI-based medical devices are subject to the safety framework established by the Medical Device Regulation (MDR), which imposes obligations on manufacturers throughout the device lifecycle. These obligations do not apply to hospitals, but they shape the regulatory requirements applicable to the devices they integrate into clinical practice. The AI Act adds a further layer of safety regulation by classifying AI-based medical devices as high-risk systems under Article 6. This is particularly relevant, as high-risk systems entail specific obligations for both AI providers and deployers, which in turn shape their behaviours and tasks. The current proposal for an EU health package would entail moving the MDR from Section A to Section B of Annex I of the AI Act.[13] This means that the AI Act would not be directly applicable, but rather that sectoral regulation would need to be updated in order to specifically address AI-based medical devices.[14] That being said, while it is unknown how the requirements of the AI Act may be translated into new medical regulation in the future, the study proceeds with the assumption that they would all maintain relevance.

II. Methods

To identify said direct liability risk, the study begins with a reconstruction of the AI deployment phases and the related possible failures of the healthcare organisation in the context of the overall socio-technical system. The identification of said deployment phases is based mainly on existing literature in the field of Health Technology Assessment (HTA), a branch of clinical engineering which provides for a structured evaluation of a technology's "clinical benefits, economic and organisational impact, as well as social, ethical and legal implications."[15] This type of assessment helps inform managerial decisions in relation to the deployment of new medical technologies.[16] Recent contributions have highlighted the need to adapt the existing HTA frameworks

[12] W. N. Price, S. Gerke and I. G. Cohen, "Liability for Use of Artificial Intelligence in Medicine" in B. Solaiman and I. G. Cohen (eds), *Research Handbook on Health, AI and the Law* (Edward Elgar Publishing Ltd 2024); *supra*, note 10.

[13] European Commission, "Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2017/745 and (EU) 2017/746 as Regards Simplifying and Reducing the Burden of the Rules on Medical Devices and in Vitro Diagnostic Medical Devices, and Amending Regulation (EU) 2022/123 as Regards the Support of the European Medicines Agency for the Expert Panels on Medical Devices and Regulation (EU) 2024/1689 as Regards the List of Union Harmonisation Legislation Referred to in Its Annex I" (2025) COM (2025) 1023 final.

[14] P. Hacker, R. Kilian and J. Costas, "Simplifying European AI Regulation: An Evidence-Based Study" (Bertelsmann Stiftung 2025) Study <https://doi.org/10.11586/2025099> (last accessed 13 May 2026).

[15] L. Sampietro-Colom and others, The AdHopHTA Handbook: A Handbook of Hospital-based Health Technology Assessment (HB-HTA) (2015) <https://www.adhophta.eu/handbook> (last accessed 13 May 2026); M. E. Uphoff and D. Krane, "Hospital-Based Technology Assessment: Essential Questions and an Operational Model" (1998) 22 Public Productivity & Management Review 60.

[16] *Supra*, note 15.

https://doi.org/10.1017/err.2026.10176

considering the specific characteristics of AI technologies, especially due to issues of data bias, human oversight, and explainability.[17] Rather than proposing a new HTA framework, this analysis systematises (through a liability-oriented perspective) the organisational decisions hospitals make when deploying AI-based medical technologies, in line with the general logic of existing HTA frameworks. To this end, literature on AI deployment in healthcare was also consulted (e.g., the lifecycle proposed by Hammer et al.[18] for AI in healthcare evaluation). Upon exploration of said deployment phases, in connection with HTA literature and applicable regulatory requirements, a variety of failures were identified.

The concept of "sphere of control" is used in this study to denote the domain of decisions and actions over which a given actor bears primary responsibility, as determined by the legal obligations that the regulatory frameworks assign to them, and which may therefore find fault-based liability when a failure within that domain contributes to harm. This notion is used descriptively to map the domain over which each actor has factual and normative influence and is distinct from how a liability regime ultimately attributes legal responsibility for a resulting harm. The two may diverge: vicarious liability, for instance, may attach to a party (the hospital) for the conduct of another (the physician) even where that conduct falls outside of the former's sphere of control. As for the reconstruction of said different spheres of control, it is based on an analysis of existing regulations, particularly the Medical Device Regulation (MDR) and Artificial Intelligence Act (AI Act), focusing on how they assign different obligations to the involved parties.

Finally, the study assesses the concrete exposure of hospitals to direct liability, by examining the structural obstacles that claimants face, as well as the circumstances under which it becomes a more realistic prospect.

III. The lifecycle of AI deployment for hospitals

It is necessary to begin by reconstructing the various phases that the hospital goes through when deploying an AI system. This is a preliminary step to identify the various failures as well as the responsibilities that are borne by the organisation, and which may in turn translate into liability if not correctly fulfilled.

The authors propose that the activities of the hospital in relation to AI deployment be broken down into a lifecycle[19] made up of five steps (Figure 1):

- Pre-procurement
- Procurement
- Integration and Implementation
- Routine use
- Suitability reassessment

Before turning to these phases, it is important to clarify the role of the AI Act. While Articles 8–15 primarily impose obligations on AI providers, Article 26 establishes specific

[17] R. Di Bidino and others, "Health Technology Assessment Framework for Artificial Intelligence-Based Technologies" (2024) 40 International Journal of Technology Assessment in Health Care e61; R. Di Bidino and others, "Unlocking AI's Value: The HTA Approach to Responsible Healthcare Integration" (2026) 2 BMJ Digital Health & AI e000250 <https://doi.org/10.1136/bmjdhai-2025-000250> (last accessed 13 May 2026).

[18] J. Hammer and others, "Navigating the Complexity of Evaluating Artificial Intelligence in Healthcare" (2025) ECIS 2025 Proceedings 11 <https://aisel.aisnet.org/ecis2025/health_it/health_it/11/> (last accessed 13 May 2026).

[19] K. N. Vokinger, T. J. Hwang and A. S. Kesselheim, "Lifecycle Regulation and Evaluation of Artificial Intelligence and Machine Learning-Based Medical Devices" in C. Shachar and others (eds), *The Future of Medical Device Regulation: Innovation and Protection* (Cambridge University Press 2022).

https://doi.org/10.1017/err.2026.10176

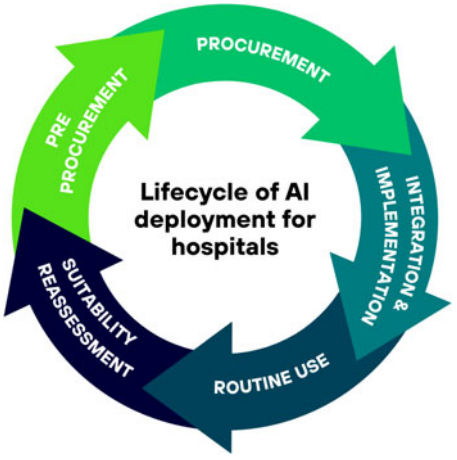


Figure 1. Cycle chart showcasing the various phases of AI deployment for hospitals.

obligations for deployers, broadly corresponding to the integration and implementation, routine use and suitability reassessment phases identified below. The pre-procurement and procurement phases therefore fall largely outside the AI Act's direct regulation of hospitals, although decisions made at these stages may affect their subsequent compliance and remain relevant to organisational fault. The MDR likewise provides an important framework for the deployment of medical devices, although its obligations are primarily addressed to manufacturers.

1. Pre-procurement

In this phase the hospital evaluates its needs and constraints in relation to the possible implementation of an AI tool.[20] The focus is on whether the deployment of an AI system is necessary, feasible and legally permissible.[21] This means, first of all, identifying which departments may be in need of and/or benefit from the implementation of AI, and for which types of tasks (e.g., administrative, diagnostics, treatment selection).

This phase also turns to the concrete capacity to accommodate this technology, such as whether the staff has sufficient training or whether there are the necessary resources to provide said training. This includes assessing the existing hardware, software and overall IT infrastructure (e.g., whether the available computers can run the software).[22]

A preliminary legal and ethical assessment is additionally included in the phase.[23] This is not yet a full due diligence review, which happens instead in the procurement phase and must be based on the concrete AI solution under consideration.

Rather, this preliminary assessment functions as an *ex ante* admissibility screening, aimed at determining whether AI systems of that general type could be integrated into the hospital at all, or whether they raise structural legal or ethical concerns that render their adoption inappropriate regardless of the specific product considered (e.g., systems designed to operate in a fully autonomous manner in high-stakes clinical decisions without the possibility of meaningful human oversight, or systems whose outputs cannot, even in

[20] *Supra*, note 15; World Health Organization, *Global Atlas of Medical Devices* (WHO 2017) <https://www.who.int/publications/i/item/9789241512312> (last accessed 13 May 2026).

[21] *Supra*, note 15.

[22] Ibid.; W. Ricciardi and G. La Torre, *Health Technology Assessment: Principi, dimensioni e strumenti* (Edizioni SEED 2010).

[23] *Supra*, note 15; J. Kim and others, "Developing a Framework for Self-Regulatory Governance in Healthcare AI Research: Insights from South Korea" (2024) 16 Asian Bioethics Review 391.

https://doi.org/10.1017/err.2026.10176

principle, be translated into reasons that clinicians can communicate to patients for the purposes of obtaining informed consent in contexts where such justification is legally and ethically required). These examples are not intended to suggest that autonomous or non-explainable systems could never yield benefits capable of outweighing their risks (e.g., triaging AI, arguably very beneficial, may not provide much time for oversight due to the nature of the task). This evaluation must therefore be conducted case-by-case. The AI Act does not directly regulate this phase, though the choices made here are still legally relevant. Introducing an AI tool into an environment lacking the infrastructure, governance or staffing necessary for safe use may constitute a foreseeable risk. The misalignment in this early stage may still constitute an organisational failure later on.

2. *Procurement*

During this phase, the hospital turns to actual concrete options to choose from. This means evaluating different competitors presenting their AI systems and choosing which one is believed to best suit the needs of the organisation.[24] Due diligence is essential during this phase, especially for what concerns appropriate equipment selection.

It includes verifying the system's regulatory status (e.g., whether it has obtained CE marking), and evaluating safety,[25] in light of criteria such as the system's robustness, accuracy, transparency and the existence of adequate human oversight measures. This assessment must also take account of the safety and performance requirements established under the MDR. The evaluation of all of these elements must be performed in line with the hospital's intended use of the tool[26] and its adequacy relative to the infrastructure and resources the hospital can put into place. Interoperability with the hospital's IT infrastructure is crucial, as well as the existence of adequate cybersecurity measures.

In evaluating these aspects, it is important for the hospital to review the documentation provided, especially the information that must be produced according to the AI Act (e.g., the intended purpose, the level of accuracy, robustness and cybersecurity, etc.; Article 13 AI Act) and the MDR's technical documentation requirements. Failure to review documentation disclosing foreseeable risks may constitute organisational negligence, as the hospital could reasonably have identified and mitigated such risks. Such conduct is in fact likely to be considered non-diligent, though it would concretely need to be assessed under the applicable national tort law; the AI Act's requirement that deployers use the system in accordance with its instructions for use (Article 26(1) AI Act) may be considered to presuppose that this documentation has been reviewed during procurement.

Contractual negotiations are part of this phase and may focus on possible duties of maintenance for the AI provider, or clauses addressing insurance, liability and other support obligations. Furthermore, this phase considers economic feasibility, in light of the cost of the purchase, as well as the costs related to updating the necessary IT resources, training the staff, putting in place the necessary governance policies and possible lawsuits for damages.[27] Ethical and legal assessments now focus more specifically on the concrete option being evaluated.[28] For example, where the preliminary phase has established that

[24] *Supra*, note 15.

[25] *Supra*, note 22.

[26] R. Tsopra and others, "A Framework for Validating AI in Precision Medicine: Considerations from the European ITFoC Consortium" (2021) 21 BMC Medical Informatics and Decision Making 274 <https://doi.org/10.1186/s12911-021-01634-3> (last accessed 13 May 2026).

[27] M. Drummond and others, *Methods for the Economic Evaluation of Health Care Programmes* (4th edn, Oxford University Press 2015); S. Landi, *Health technology assessment (HTA): uno strumento a supporto delle decisioni manageriali nelle aziende sanitarie* (Giappichelli 2021); *supra*, note 15.

[28] Ibid.; *supra*, note 22.

https://doi.org/10.1017/err.2026.10176

only systems which allow for effective human oversight may be considered, the following procurement phase assesses whether the specific AI device under evaluation actually enables such oversight in practice (e.g., whether clinicians can meaningfully review and, if necessary, disregard its outputs).

3. Integration and implementation

It is in this phase that the hospital, after having procured the AI, determines how to actually integrate it with the existing IT infrastructure and implement it ensuring that the AI can operate within the hospital's environment.[29]

It significantly entails deciding how the AI is to be employed in the workflows of healthcare professionals,[30] and specifically of physicians when it comes to CDSSs. Hospitals must determine at which point of the clinical process the AI will be used and how clinicians are expected to interact with it. Depending on the elaborated workflow, the hospital also assigns certain staff to employ the AI and, in particular, identifies who must exercise oversight over it (Article 26(2) AI Act). The hospital may put in place a quality management system, envisioning opportunities, possible risks, and relevant indicators for each. This entails defining protocols to apply if failures occur, as well as incident-response procedures for reporting and handling AI malfunctions or unexpected behaviours (Article 26(5) AI Act). This is essential to ensure that tasks are correctly assigned and that accountability is established.

Where necessary, the hospital will set up the necessary training for the involved staff[31] (Article 4 AI Act), following the provision of information to workers' representatives and affected workers that they will be subject to the use of high-risk AI (Article 26(7) AI Act). It will implement the necessary governance requirements by setting up, for example, an AI board and defining internal AI policies. The hospital must also adopt governance procedures for logging, monitoring and documenting the system's functioning (Article 26(6) AI Act).

This phase may entail a pilot/testing phase, before deployment is more largely put into place, to ensure that possible risks are detected early and addressed.[32] Failure to test adequately may be regarded as an organisational oversight.

While, as seen, the AI Act establishes certain requirements for some of these activities through Articles 4 and 26, compliance with them cannot be assumed to exhaust the hospital's duty of care. Rather, they can provide a minimum benchmark for assessing diligence, with additional measures potentially required depending on the circumstances.

4. Routine use

During this phase, the use of the AI tool becomes part of regular clinical practice, for the departments that it was provided to. The hospital continuously monitors the deployment of the AI to detect whether any risks, malfunctions, or unexpected behaviours manifest (in accordance with the principles of a quality management system).[33]

[29] S. Reddy and others, "Evaluation Framework to Guide Implementation of AI Systems into Healthcare Settings" (2021) 28 BMJ Health & Care Informatics e100444 <https://doi.org/10.1136/bmjhci-2021-100444> (last accessed 13 May 2026); *supra*, note 18; *supra*, note 20.

[30] H. J. Marcus and others, "The IDEAL Framework for Surgical Robotics: Development, Comparative Evaluation and Long-Term Monitoring" (2024) 30 Nature Medicine 61.

[31] Y. Xu and others, "Medical Education and Physician Training in the Era of Artificial Intelligence" (2024) 65 Singapore Medical Journal 159.

[32] *Supra*, note 15.

[33] *Supra*, note 23.

https://doi.org/10.1017/err.2026.10176

The hospital also monitors physician behaviour, meaning how they employ the AI, whether they understand its outputs, and whether use patterns indicate automation bias, under-reliance or misuse. This includes responding to complaints raised by healthcare professionals and patients. Wherever necessary, the hospital implements corrective actions and process enhancements affecting workflows, policies, and documentation, ensuring all organisational standards are aligned with identified quality objectives. The hospital may need to flag issues to the AI provider and enforce contractual obligations relating to maintenance, support or system performance where necessary.

Training must continue to be administered, as it is not a one-time activity but requires constant updating, and new employees may enter the organisation.[34]

During this phase, updates may be introduced by the AI provider. It is up to the hospital to evaluate whether these updates require changes to workflows or policies and to ensure that updates are correctly implemented in the hospital's environment.

Hospitals may have to handle incidents during this phase and report them where necessary (Article 26(5) AI Act). Legal actions may be brought against the physicians and/or the hospital, under the applicable national liability rules, where the relevant conditions are met, as a result of the use of the AI system, and the hospital must be prepared to respond accordingly.

Legal and ethical assessment[35] must continue, as new norms or ethical standards may emerge over time, or as monitoring of the AI may reveal issues that previously went undetected.

Furthermore, the hospital assesses whether the AI is complying with overall plans, whether it meets the needs identified in the pre-procurement phase, and whether it functions as expected across different clinical contexts or patient groups.

5. Suitability reassessment

This phase entails assessing the technology in a more long-term perspective, after the AI system has been fully integrated and deployed. The hospital evaluates how the system behaves over time and whether it continues to operate safely, effectively, and in alignment with institutional objectives.[36] This means analysing information collected over time, especially incidents, recurring complaints, and other documented anomalies, in order to identify possible patterns or emerging risks.[37] This applies in particular to the physician–AI relationship and whether problematic interaction patterns develop. It is essential to examine whether the performance of the AI changes over time, and specifically whether it worsens or drifts, as corrective measures may be required.[38] Over time, new updates and models may be released, and technological developments may render earlier versions of the AI system obsolete or "unsafe" compared to the current state of the art.[39] The hospital must evaluate whether updates should be adopted, and whether they require changes to established workflows or policies.[40]

The hospital performs evaluations on whether the AI continues to meet the objectives, including whether it remains cost-effective given the burdens that it entails. The hospital

[34] *Supra*, note 31.

[35] *Supra*, note 18.

[36] *Supra*, note 22; *supra*, note 18.

[37] *Supra*, note 23.

[38] D. Vela and others, "Temporal Quality Degradation in AI Models" (2022) 12 Scientific Reports 11654.

[39] J. Feng and others, "Clinical Artificial Intelligence Quality Improvement: Towards Continual Monitoring and Updating of AI Algorithms in Healthcare" (2022) 5 NPJ Digital Medicine 66 <https://doi.org/10.1038/s41746-022-00611-y> (last accessed 13 May 2026).

[40] K. Lekadir and others, "FUTURE-AI: International Consensus Guideline for Trustworthy and Deployable Artificial Intelligence in Healthcare" (2025) 388 BMJ e081554.

https://doi.org/10.1017/err.2026.10176

may come to the decision to retire the AI tool and will then have to put in place the necessary measures to ensure that it is safely decommissioned[41]; failure to retire unsafe technologies may constitute a breach of the hospital's organisational duties.

IV. Possible failures and liability

European courts traditionally recognise that hospitals have obligations to ensure safe facilities, equipment and organisational conditions.[42] In particular, this encompasses an appropriate selection of technologies and staff, as well as adequate supervision, proper training of the staff, safe implementation of workflows and protocols, adequate maintenance, and more.[43]

These obligations are not changed per se by the introduction of CDSSs but rather need to be recontextualised as new risks are introduced, that go beyond those that are typically presented by traditional medical devices.

Direct liability may be borne by healthcare organisations, namely hospitals, whenever they engaged in faulty behaviour, and said conduct is causally connected with the harm suffered by the patient. This fault-based liability can be traced back to the hospital's breach of an organisational duty.[44]

The lifecycle presented in section III illustrates a wide variety of organisational decisions that hospitals must make when deploying AI systems, and for which, if harm is caused, hospitals could bear direct liability, though not all of those choices may be relevant. There are a variety of cross-cutting organisational errors, that may occur, and which may lead to liability.

1. Organisational unreadiness: The hospital procured and deploys a CDSS without adequate infrastructure, staffing, governance structures and overall resources that would ensure a safe operation.[45]
2. Deficient due diligence: The hospital failed to verify the system's regulatory status, robustness or transparency during procurement, and/or it failed to review documentation disclosing foreseeable risks (Article 13 AI Act; relevant MDR technical documentation requirements).[46]
3. Inadequate input data: The hospital has failed to ensure that the input data (meaning "data provided to or directly acquired by an AI system on the basis of which the system produces an output," Article 3(1)(33) AI Act) which has been fed into the AI system is relevant and sufficiently representative of the relevant patient groups (Article 26(4) AI Act).[47]
4. Clinical setting misalignment: The hospital has erroneously defined the clinical context in which to insert the CDSS, such as the department(s), the stage of the clinical pathway, or the patient groups for which the system is intended.[48]
5. Flawed clinical workflow: The hospital has designed or maintained clinical workflows[49] that do not allow for adequate physician/machine interaction, as they

[41] *Supra*, note 15.

[42] D. Giesen, *International Medical Malpractice Law: A Comparative Study of Civil Responsibility Arising from Medical Care* (Brill Nijhoff 1988).

[43] *Supra*, note 10.

[44] *Supra*, note 10; *supra*, note 42.

[45] *Supra*, note 15; D. F. Sittig and H. Singh, "A New Sociotechnical Model for Studying Health Information Technology in Complex Adaptive Healthcare Systems" (2010) 19 Suppl 3 Quality & Safety in Health Care i68.

[46] *Supra*, note 15; *supra*, note 22.

[47] *Supra*, note 40.

[48] *Supra*, note 26; *supra*, note 29; *supra*, note 40.

[49] *Supra*, note 45.

https://doi.org/10.1017/err.2026.10176

may not allow for effective use and/or oversight.[50] Inadequate time allocation may be relevant.

6. Ineffective oversight measures: The hospital has not put in place measures to ensure human oversight that is effective, timely, and competent, including unclear or impracticable assignment of oversight responsibilities and inadequate explainability measures (Articles 26(2) and 14 AI Act).[51]
7. Staff competency gaps: The hospital has not ensured that all relevant staff members possess and maintain the required competences for safe use of the CDSS. This goes not only for initial training, but also for continuous learning and training of new personnel (Articles 4 and 26(7) AI Act).[52]
8. Fragmented communication flows: The hospital has not set up communication flows that allow for safety-critical information to reach the appropriate individuals or units (e.g., systems to flag anomalies).[53]
9. Technical environment mismatch: The hospital has inadequately configured or integrated the CDSS within its own IT infrastructure.[54]
10. Deficient monitoring and surveillance: The hospital has not put in place the necessary processes for adequate monitoring and surveillance over the CDSS's behaviour and/or its use by physicians (e.g., for automation bias, under-reliance, or misuse) (Article 26(5) AI Act).[55]
11. Unsafe update and change-management processes: The hospital has failed to manage safely relevant updates or changes to the CDSS. This may consist of failing to implement necessary updates, or doing so without adequate testing, training, or modifications to policies, governance, workflows, and more.[56]
12. Substandard incident and safety management: The hospital has failed to detect and/or respond to incidents linked to the CDSS. The hospital has failed to create adequate reporting mechanisms and to implement corrective measures (Articles 26(5) and 73 AI Act).[57]
13. Neglect of traceability and record keeping: The hospital has failed to keep the generated logs and maintain adequate documentation and records. This may impair both safety and post-incident reconstruction (Article 26(6) AI Act).[58]
14. Inadequate periodic reassessment of system suitability: The hospital has not periodically re-evaluated whether the CDSS remains clinically and organisationally appropriate, and/or has not retired/replaced systems that have become unsuitable.[59]

The failures that have hereby been identified are cross-cutting, as they may arise in different stages of the deployment lifecycle, as shown in Figure 2. Of course, the mere existence of one (or more) of these organisational errors does not immediately point to liability. These must be understood as situations that may acquire relevance when

[50] European Data Protection Supervisor, *TechDispatch – Human Oversight of Automated Decision-Making* (Publications Office of the European Union 2025).

[51] Ibid.

[52] *Supra*, note 31; *supra*, note 27.

[53] *Supra*, note 45.

[54] Medical Device Coordination Group, *MDCG 2023-4: Medical Device Software (MDSW) – Hardware Combinations* (2023).

[55] *Supra*, note 38; *supra*, note 45.

[56] *Supra*, note 40; *supra*, note 38; *supra*, note 39.

[57] M. Chatzipanagiotis, "Incident Reporting and Investigation Under the AI Act: Some Insights from Aviation" (2026) 34 International Journal of Law and Information Technology eaaf019.

[58] *Supra*, note 40.

[59] *Supra*, note 39; *supra*, note 18.

https://doi.org/10.1017/err.2026.10176

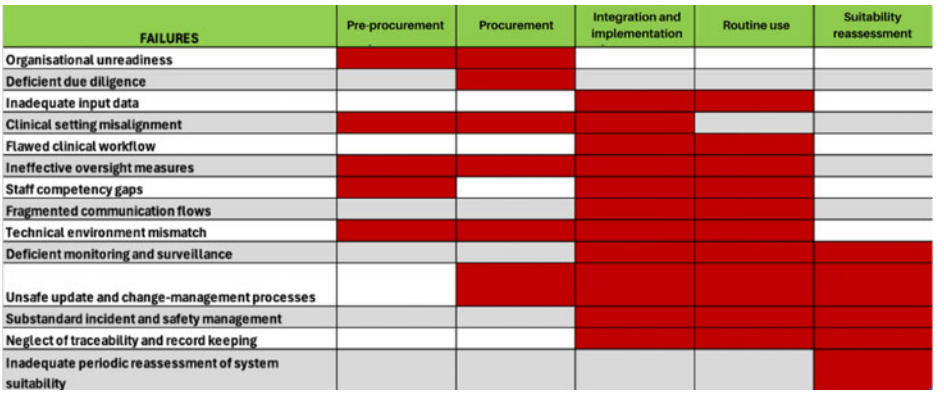


Figure 2. Chart showing the stages of the lifecycle where each of the listed organisational failures may occur.

evaluating the diligence of the hospital, and only when they can be reconnected to the harm suffered by the patient.

The lifecycle remains an important analytical tool, as it makes it possible to locate the point of origin of a failure. This is particularly relevant as the assessment of foreseeability, and therefore fault, may vary depending on the stage at which said failure occurs. On top of that, early omissions may shape later failures. For example, wrong choices made at earlier stages may create latent conditions that constrain later conducts. It is important to consider whether there is only one failure at an early stage, which then constrained further decisions, or whether multiple ones have occurred. In Figure 2, each failure is mapped to the stages where it may originate.

V. Spheres of control

After having mapped the organisational failures that may give rise to direct hospital liability, it is necessary to consider the broader picture of interacting responsibilities. The same clinical environment that the hospital's choices help to create is also shaped upstream by the AI provider and, downstream, it constrains the healthcare professionals' activities. To determine which party may bear direct liability for a given harm it is thus necessary to identify which sphere of control the relevant failure falls within.[60] As used here, a "sphere of control" refers to the domain of decisions and actions over which a given actor bears primary responsibility. Where those domains overlap, the spheres are within "shared domains." Liability may thus attach to one or more party depending on where exactly the failure(s) occurred.

1. Interaction between hospital and AI provider

It must be noted that the clinical care environment in which the physician operates is shaped both by the hospital and by the AI provider.[61] These parties have certain complementary obligations and thus constitute "shared domains" between the two (see Figure 3). The following paragraphs trace the main shared domains, showing how each creates a zone of overlapping responsibility whose attribution depends on where the failure lies exactly.

[60] C van Dam, *European Tort Law* (Oxford University Press 2007).

[61] J L Davis, ""Affordances" for Machine Learning" (2023) Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency 324.

https://doi.org/10.1017/err.2026.10176

AI PROVIDER CONTROL	SHARED DOMAIN	HOSPITAL CONTROL
Interoperability and compatibility provision	TECHNICAL INTEGRATION	IT infrastructure integration
Intended use definition	DEPLOYMENT CONTEXT	Clinical deployment context definition
Transparent disclosure of relevant information	PROCUREMENT	Due diligence reviews and system verifications
Dataset representativeness and disclosure of training limitations/biases	DATA RELEVANCE AND QUALITY	Provision of adequate input data
In-system workflow constraints definition	WORKFLOW	Clinical workflow set-up
Oversight measures provision (logs, alerts, etc.)	OVERSIGHT	Staff assignment and oversight conditions
Documentation and training materials provision	TRAINING	Training delivery
Update release and accompanying information provision	UPDATE	Update implementation
Post-market surveillance and post-incident measure implementation	INCIDENT MANAGEMENT	Monitoring and incident response
Automatic logging and interpretability tools	DOCUMENTATION AND TRACEBABILITY	Secure storage of logs and documentation

Figure 3. Chart showing the spheres of control of the hospital and of the AI provider (non-comprehensive list).

Consider, for example, the technical integration of the AI system in the hospital. The AI provider works on the compatibility and interoperability of the system (Annex I, point 14.5 MDR; MDCG 2023-4[62]), but it is then the hospital that has to set up the necessary resources and architectures to actually integrate the technology within its IT infrastructures.[63]

Similarly, the deployment context is jointly defined: the producers define the intended purpose of the system (Article 5 MDR), but then it is the hospital that actually has to use it according to the information for use (Article 26(1) AI Act) and assign it to the adequate department and staff for the correct scopes.[64] Even before this stage, the procurement process itself functions as a shared domain. The AI provider is legally mandated to provide transparent documentation on a system's capabilities and risks (Article 13 AI Act, Annex I,

[62] *Supra*, note 54.
[63] *Supra*, note 45.
[64] *Supra*, note 26.

https://doi.org/10.1017/err.2026.10176

point 23.4 MDR), while the hospital must perform a due diligence review and verify the characteristics of the AI system.[65]

Furthermore, ensuring data relevance and quality is also a joint responsibility. The hospital exercises control over the clinical input data fed into the CDSS (Article 26(4) AI Act), though the efficacy of said data depends on the AI provider's initial design and the transparency of the training datasets used.[66]

This is true for workflows as well. Hospitals can define said workflows through internal policies,[67] though some AI systems may by-design impose a certain level of automation.[68]

Similarly, oversight is an obligation that is addressed to both deployers (i.e., the hospital) and AI providers (i.e., the producers/vendors of the AI) under the AI Act (Articles 14 and 26 AI Act). In many ways, these obligations are complementary, so if the providers of the AI do not set up adequate oversight measures in the design of their system, the hospital may not be able to ensure effective oversight, despite its best efforts. This of course goes the other way too: oversight may be ineffective, but it is not necessarily due to a product defect, and it may instead be the hospital that failed to set up the necessary conditions to ensure that said oversight measures can be employed.[69] Where a product defect arises, and said defect is causally connected with harm suffered by the patient, the producer of the AI system may be liable under product liability law.

Training is another partially shared responsibility (though to a lesser extent), as the AI provider may have to provide adequate information on the AI system that allows physicians to adequately use the technology. It is of course up to the hospital to actually provide the training[70] (Article 26(2) AI Act) but where lacking the necessary information about the AI system from the AI provider (mandatory under Article 13(3)(b)(vii) AI Act), it may not prove effective. The obligation to provide adequate AI literacy, which applies to both providers and deployers, may also be relevant in this sense (Article 4 AI Act).

Updates to the AI system have to be supplied by the AI provider with adequate information (Article 13(3)(e) AI Act), but while the hospital is not necessarily required to implement every update, updates addressing errors or safety issues may need to be implemented to ensure the continued safe and compliant functioning of the system. So, if harm is traced back to an update, both the producer and the hospital are potentially liable parties, and it will be necessary to identify where exactly the failure occurred.

Incident management is split as well. The AI provider has to continuously surveil the product and implement adequate procedures for their reporting (Articles 83 and 87 MDR) and must implement measures to remedy the incidents and prevent future ones (Articles 17(1)(i), 72 and 73 AI Act).[71] The hospital is in a surveillance position and has to flag incidents where they occur (Articles 26(5) and 73 AI Act) and implement changes to its own organisation measures to address the incidents and prevent them where necessary.[72]

Documentation and traceability constitute another shared domain of responsibility. The hospital has the legal obligation of maintaining logs of the system's functioning (Article 26(6) AI Act), though this obligation can only be fulfilled if the AI provider has integrated the necessary technical logging capabilities and provided clear instructions on how to interpret and store said data (Article 13 AI Act).[73]

[65] *Supra*, note 15; *supra*, note 22.

[66] *Supra*, note 40.

[67] *Supra*, note 45.

[68] M. R. Endsley, "Level of Automation Forms a Key Aspect of Autonomy Design" (2018) 12 Journal of Cognitive Engineering and Decision Making 29.

[69] *Supra*, note 50.

[70] *Supra*, note 31.

[71] *Supra*, note 57.

[72] Ibid.

[73] *Supra*, note 40.

https://doi.org/10.1017/err.2026.10176

It must be noted that both the hospital and the AI provider have a significant role in designing the clinical care environment in which the physician then operates. Of course, it is first the provider of the AI that sets some boundaries in designing the system,[74] but it is then up to the hospital to build on those boundaries and further design the environment. Furthermore, even after the clinical environment is set up, there are some further obligations to both the AI provider and the hospital that focus around the same topics. It is fundamental to acknowledge this situation, as one party's sphere of control may limit the other's. This may in turn have an effect on the liability risk borne by each.

It is important to highlight that the hospital is in this context being considered for potential organisational fault. The AI provider can instead be considered liable according to product liability (which is strict) as a relevant "economic operator" (see the new Product Liability Directive), or under national fault liability regimes.[75] This study does not go in depth on the AI provider's liability, as it is outside of its scope, and considers the "provider" as a sole party, for the sake of simplicity, despite the fact that in reality there may be a variety of potentially liable parties on the technical side (authorised representatives, importers, etc., see Article 8 PLD).

2. *Interaction between hospital, AI provider and healthcare professional*

Healthcare professionals (and particularly physicians) may be limited by the clinical environment designed by both the AI system producer and the hospital. When performing their tasks, they do not operate in a vacuum, but rather within pre-set circumstances. As such, the physician's sphere of control is necessarily limited within those boundaries.[76] As seen in the introduction, while usually we tend to think of errors in relation to the humans that caused them,[77] it is often the overall system they operate in that has the most potential to be improved and to prevent harm.[78]

That being said, physicians remain of course bound by their own obligations to the patient, that Member States tend to qualify as either contractual or extra-contractual in nature.[79] Physicians must still provide care following the requirement of professional diligence.

Hospitals must ensure that the clinical environment is set up in a way that allows physicians to meet their professional obligations. When it comes to CDSSs specifically, this is especially about setting up the appropriate workflow, providing adequate staffing, and allocating adequate timing and training.[80] All of these circumstances are essential to ensure that the physician can use the AI tool in an effective manner, especially as concerns the oversight.[81] If these conditions are not met, physicians may be placed in a situation where it is practically impossible to correctly perform their tasks and to exercise adequate oversight.[82]

The courts may, in certain cases, consider the harm to be primarily caused by organisational failures, and that the physician was not in the position to comply with their professional obligation. Such an assessment would be made under the applicable national

[74] *Supra*, note 61.

[75] P. Hacker, "The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future" (2023) 51 Computer Law & Security Review 105871.

[76] *Supra*, note 61.

[77] *Supra*, note 8.

[78] *Supra*, note 10.

[79] H. Nys, "Report on Medical Liability in Council of Europe Member States: A Comparative Study of the Legal and Factual Situation in Member States of the Council of Europe" (Council of Europe 2005) CDCJ (2005) 3 rev1.

[80] *Supra*, note 31; *supra*, note 45.

[81] *Supra*, note 50.

[82] *Supra*, note 1.

https://doi.org/10.1017/err.2026.10176

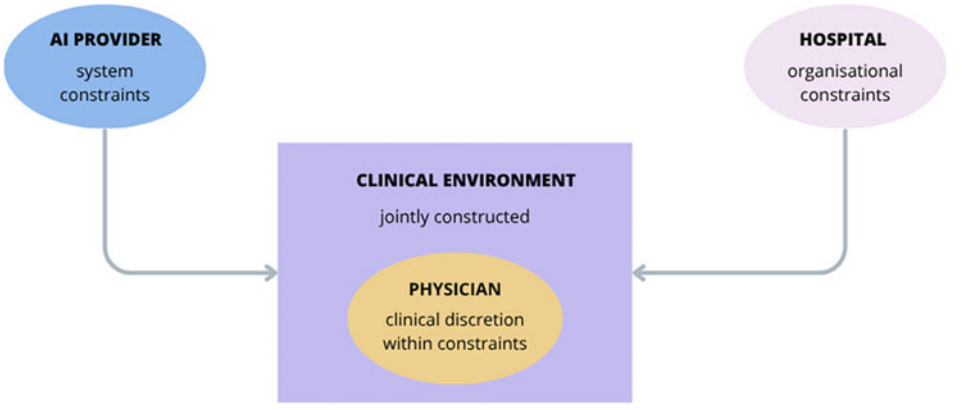


Figure 4. Chart displaying the spheres of control of the AI provider, of the hospital, and of the physician.

regime, particularly its rules on causation, taking into account whether the organisational conditions created by the hospital prevented the physician from meeting the applicable standard of professional diligence. On the other hand, if the hospital does provide all necessary infrastructures, resources, training, correctly designed workflows, etc., the physician could not rely on organisational shortcomings to excuse their negligence. It is therefore essential to consider how the hospital's and the physician's spheres of control interact, and in particular how one may limit the other. Of course, a physician cannot be held liable for aspects over which they had no control, and vice versa. At the same time, it remains true that harm may result from multiple concurrent causes, meaning that the identification of one party's liability does not automatically exclude that of another.

The constraints on physicians put in place by the hospital are of course summed with those of the AI providers, coherently with the hospital/provider relationship presented in the previous paragraph. On this point, see Figure 4.

VI. Concrete exposure to risk

It has been highlighted, so far, what failures the hospitals could incur in, as well as their responsibilities in setting up the overall clinical environment. From a concrete standpoint, however, the direct liability risk of hospitals may be limited. It is necessary to be aware that a number of obstacles can reduce the likelihood that direct hospital liability could be successfully invoked.

First, organisational failures tend to be "invisible": organisational failures often occur long before the harm materialises (consider in particular the failures in the first three deployment stages), and they rarely leave a clear trail.[83] Establishing the causal link between an organisational failure and the concrete injury suffered by a patient is therefore quite difficult. Factual causation follows the "but for" test,[84] meaning that it requires showing that, but for the hospital's failure, the harm would not have occurred. Where the AI system and the physician also contributed to the outcome, attributing the harm to the hospital's organisational conduct can represent a demanding task. The same goes for

[83] *Supra*, note 10.

[84] M. Infantino, "Unravelling Causation in European Tort Laws: Three Commonplaces through the Lens of Comparative Law" (2019) 83 Rabels Zeitschrift für ausländisches und internationales Privatrecht 647; J. Kleinschmidt, "Causation" in J. Basedow, K. J. Hopt and R. Zimmermann (eds), *The Max Planck Encyclopedia of European Private Law* (Oxford University Press 2012).

https://doi.org/10.1017/err.2026.10176

normative attribution[85]: a court must conclude that the risk which materialised was precisely the kind of risk that the hospital's duty was meant to guard against, and that it fell sufficiently within the hospital's sphere of control to found liability. In AI-related harm, this determination may be contested.

A further obstacle is that hospitals have control over most of the information that would be necessary to establish an organisational failure claim (e.g., logs, incident reports, due diligence reviews, etc.). With the Artificial Intelligence Liability Directive (AILD) proposal being scrapped by the EU,[86] the mechanisms of disclosure of evidence and presumptions that it would have provided for are now out of reach.[87] It is up to national laws to provide for burden of proof mechanisms that can favour claimants seeking compensation for AI-related harm, though some legal systems may already provide for rules that favour claimants acting against hospitals instead. For example, Italian law subjects healthcare facilities to contractual liability, with the burden of proving proper performance falling on the defendant.

Finally, medical harm may be primarily attributed to individual physician negligence in liability claims, while hospital liability is more commonly pursued through vicarious liability than on the basis of the hospital's own organisational failures.[88]

Under certain circumstances, however, a direct liability claim may be more successful. Consider, for example, the case where the failure is not latent but rather has been flagged and openly disregarded (e.g., incident reports documented systematic misuse of the CDSS). In these cases, the foreseeability of harm may be easier to establish, and the failure becomes more "visible." Where the hospital's regulatory obligations as a deployer under the AI Act have been breached (e.g., failure to designate competent oversight personnel (Article 26(2) AI Act)), claimants also benefit from a clearer benchmark for the evaluation of the hospital's conduct. Moreover, repeated failures are also more likely to attract direct liability, in contrast with more isolated incidents.

VII. Conclusions

It is important to consider hospital liability beyond just the paradigm of vicarious liability for the healthcare professional's conduct. The hospital has its own responsibilities for what concerns the implementation of new healthcare technologies, which must be even more carefully carried out when it comes to AI systems. In this sense, the hospital may bear its own direct liability risk and must as such be considered carefully as a possibly liable party, especially since organisational failures are often the aspect that can go through most improvements. To this end, it is crucial to consider the lifecycle of AI deployment which, as proposed by the authors, follows five phases: (1) pre-procurement; (2) procurement; (3) integration and implementation; (4) routine use; (5) suitability reassessment. At each of these steps, the hospital must engage in delicate choices, which, if performed incorrectly, may result in failures and possibly in organisational fault.

The choices performed by hospitals are often tightly correlated with the decisions taken by the providers of the AI system. Some domains are "shared" between the two, and as such adequate implementation of certain measures (e.g., oversight measures) depends on both. AI provider and hospital, in particular, define the clinical environment within which the physician operates. This means that physicians' clinical discretion is naturally limited

[85] Ibid.

[86] Commission, "Commission Work Programme 2025: Moving Forward Together – A Bolder, Simpler, Faster Union" COM (2025) 45 final.

[87] P. Hacker, *Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence: Complementary Impact Assessment* (European Parliamentary Research Service (EPRS) 2024).

[88] *Supra*, note 10.

https://doi.org/10.1017/err.2026.10176

within said environment. These considerations are essential as they help define the boundaries in the spheres of control of each actor, which can then have an influence as to liability allocation.

Finally, it must be considered that the concrete exposure of hospitals to direct liability could remain limited in practice. Organisational failures tend to be latent, causally difficult to isolate, and routinely eclipsed by the individual-negligence framing. That said, liability becomes a more realistic prospect where the hospital has breached specific AI Act obligations and where incident-response records reveal flagged-and-disregarded risks.

Competing interests. The authors declare none.

Cite this article: C Giorgetti, G Contissa, and A Giorgetti, "Hospitals as AI Deployers: Organisational Failures and Direct Liability Risks". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2026.10176

https://doi.org/10.1017/err.2026.10176