Indian J Med Ethics Vol XI (Cumulative Vol XXXIV) No 4 Oct-Dec 2026

THEME: RECLAIMING HUMAN AGENCY IN THE AGE OF HEALTH-AI

COMMENTARY

Artificial intelligence in pre-hospital emergency medicine in Israel: Ethical and legal considerations

ROTEM WAITZMAN, MOSHE Z ABRAMOWITZ

Abstract

Artificial intelligence (AI) is rapidly transforming pre-hospital emergency medicine (PHEM). In Israel, systems already deployed at Magen David Adom and hospitals such as Sheba Medical Center, Ichilov Hospital, and Barzilai Medical Center demonstrate AI's potential to improve triage, despatch, and emergency preparedness. Yet, this accelerated adoption has outpaced ethical, legal, and institutional safeguards. This commentary analyses the governance challenges of AI in Israeli PHEM — focusing on informed consent, data ownership, bias, liability, oversight, and public trust — and proposes practical recommendations for responsible implementation.

Six critical gaps are identified: (1) absence of patient-centred consent mechanisms; (2) fragmented data ownership and vendor dependence; (3) lack of equity audits; (4) unresolved liability standards; (5) insufficient institutional oversight; and (6) limited public consultation. These gaps pose immediate risks for patients and long-term threats to trust and legitimacy. To address these challenges, we propose the establishment of AI ethics committees, transparent consent protocols, a national data governance framework, mandatory fairness audits, clarified liability rules, and structured public engagement. Israel's experience underscores the need to build ethical frameworks in parallel with technological innovation, offering lessons for other healthcare systems seeking to balance innovation with accountability and patient rights.

Keywords: *artificial intelligence, pre-hospital emergency medicine, ethics, consent, governance, liability, trust*

Introduction

Artificial intelligence (AI) technologies are increasingly integrated into healthcare systems, including pre-hospital emergency medicine (PHEM), where rapid decision-making and patient vulnerability amplify both opportunities and ethical challenges [1, 2]. In Israel, emergency services and hospitals have already begun deploying AI decision-support tools: Magen David Adom (MDA), the national medical emergency, disaster, ambulance and blood service introduced AI-assisted triage and ambulance despatch, Sheba Medical Center developed predictive monitoring for cardiac events during transport, Ichilov Hospital implemented trauma dashboards linking paramedic and hospital data, and Barzilai Medical Center used AI-enhanced despatch during *Operation Iron Swords,* the invasion of Gaza in October, 2023 [3, 4, 5, 6]. These applications demonstrate clear clinical potential for optimising triage, improving outcomes, and strengthening preparedness under extreme time constraints.

Yet, the integration of AI also raises complex ethical, legal, and governance concerns. Key questions relate to secondary use of clinical data, informed consent under emergency conditions, algorithmic bias, accountability, liability, and public trust [7, 8]. While international frameworks such as the World Health Organization (WHO) [9], United Nations Educational Scientific and Cultural Organization (UNESCO) [10], and the European Union Artificial Intelligence Act (EU AI Act) (2024) offer guidance, Israeli regulation remains fragmented, with no comprehensive national framework for AI oversight in PHEM.

This paper examines these dilemmas in the Israeli context, offering a normative and theoretical analysis grounded in real-world developments. Its aim is to identify the principal governance gaps and propose practical recommendations to support responsible and trustworthy AI deployment in emergency care.

Background and current developments in PHEM AI in Israel

The integration of AI into Israel's PHEM has advanced rapidly, supported by national innovation initiatives and institutional projects. MDA developed AI-based triage and despatch tools using retrospective Emergency Medical Service (EMS) data [3, 4], while hospitals have piloted preparedness systems. For example, during *Operation Iron Swords* beginning in 2023, Beilinson Medical Center deployed an AI system to monitor mass-casualty events and coordinate resources [11].

Despite this progress, most systems rely on clinical data originally collected for treatment, without explicit patient consent for secondary use. Data ownership remains fragmented, with no national framework for sharing between EMS, hospitals, and vendors, creating regulatory ambiguity over privacy and accountability. Current laws, such as the Israeli Privacy Protection Law, 1981, were not designed for continuous AI training or operational deployment, and ethics committees focus on research rather than real-time applications.

Although global guidelines exist [9, 10], as also the EU AI Act, 2024, Israel has not systematically adopted them. Institutions therefore act independently, often without national oversight, public engagement, or dedicated governance frameworks.

AI application in PHEM in Israel: At a glance

AI in Israel's PHEM has quickly progressed from pilots to operational use. Hospitals and national EMS employ AI for triage, despatch, trauma assessment, and mass-casualty response [3, 4, 5, 6]. These deployments not only highlight clinical promise, but also expose governance, ethical, and legal gaps that lag behind innovation [1, 2, 9].

This section reviews six domains of concern — informed consent, data governance, bias, liability, oversight, and public trust — identifying gaps in Israeli practice and proposing recommendations for responsible AI integration.

1. Informed consent and secondary data use

Ethical gap

The deployment of AI systems in Israeli PHEM relies heavily on secondary use of patient data originally collected for clinical and operational purposes. For instance, Magen David Adom's AI-powered triage system is trained on retrospective EMS call and despatch data [12], and Sheba Medical Center[a] has developed predictive ambulance-transfer models using real-time patient vital signs [3,4]. Similarly, Ichilov Hospital's[b] trauma dashboard integrates structured paramedic reports with hospital data streams [5], while Barzilai Hospital[c] employed AI-integrated despatch systems during *Operation Iron Swords,* to optimise mass-casualty coordination [6].

Although AI applications show clear clinical promise, patients rarely give explicit consent for their data to be reused for algorithm training, recalibration, or vendor collaborations. No mechanisms exist for retrospective or real-time consent, leaving patients subject to AI-driven decisions without knowing that their data sustains these systems [7]. In emergency settings — where informed consent is already difficult — this lack of transparency heightens concerns over autonomy, ownership, and public trust [1, 8].

Recommendation

To address these concerns, Israeli EMS providers and hospitals should develop patient-centred transparency and consent frameworks adapted to the unique constraints of emergency care. These could include:

- *General disclosures at admission:* Hospitals and EMS organisations could inform patients and families, upon entry into the system, that AI technologies may be used in clinical decision-making and that data may contribute to continuous system learning.
- *National-level communication campaigns:* Public information initiatives could clarify the role of AI in pre-hospital emergency medicine, emphasising both benefits (eg, faster triage, improved outcomes) and risks (eg, data reuse, bias).
- *Family engagement protocols:* Where feasible — such as in non–life-threatening situations, inter-facility transfers, or when family members are present and time allows — emergency providers should communicate with families about AI-supported interventions, making explicit that ongoing data input may be used for continuous algorithmic improvement. In contrast, during immediate life-saving interventions (eg, cardiac arrest resuscitation, mass-casualty triage, or situations involving unconscious patients without available surrogates), real-time communication may not be practicable and should instead be supplemented by post-event disclosure mechanisms.

By adopting these measures, institutions would proactively respect patient autonomy, enhance transparency, and foster legitimacy for AI deployment in emergency contexts [2, 9, 10]. Importantly, clarity is also needed about whether patients are offered the choice to opt out of AI applications, and how such preferences could be balanced against system-wide efficiency and equity considerations [13].

2. Data ownership, privacy, and governance

Ethical gap

Israel's fragmented healthcare structure creates ambiguity regarding data ownership and governance for AI in PHEM. MDA controls EMS call data, Sheba develops predictive monitoring, Ichilov manages trauma dashboards, and Barzilai used AI dispatch during *Operation Iron Swords* [3, 4, 5, 6].

No national framework regulates data sharing or reuse, and vendor partnerships often involve proprietary models trained on Israeli data, without clear agreements on institutional or patient rights [1, 14]. Existing law, such as the Privacy Protection Law (1981), does not address large-scale aggregation or continuous AI updates, leaving institutions with "black box" systems they cannot fully audit — undermining accountability and safety.

Recommendation

To strengthen governance and protect patient rights, Israel requires a coordinated national data governance strategy specifically addressing AI in healthcare. Key measures should include:

- *Unified national standards* clarifying data ownership, patient rights, and vendor obligations in AI development and deployment.
- *Cross-institutional data-sharing frameworks* that allow EMS providers, hospitals, and research centres to collaborate while ensuring security, privacy, and transparency.

- *Vendor accountability mechanisms,* including legally binding contracts requiring clarity, auditability, and data protection safeguards.
- *External oversight* in the form of independent audits of AI models and data practices, ensuring compliance with privacy standards and ethical norms [9, 10].

By implementing such governance structures, Israel could move from fragmented, institution-specific arrangements toward a system that balances innovation with patient protection and public trust. Without this shift, AI in PHEM risks perpetuating a patchwork of practices that privilege institutional and vendor interests over the collective good.

3. Algorithmic bias and justice

Ethical gap

AI in Israeli PHEM is trained on datasets that reflect existing service use, rather than full population diversity. MDA relies on retrospective EMS calls, while Sheba and Ichilov use their own hospital records [3, 4, 5, 12]. These records typically include electronic health records, triage classifications, diagnostic codes, vital signs, and documented clinical outcomes. As such, they reflect patterns of care among patients who accessed emergency services, rather than the broader population, potentially embedding pre-existing disparities into algorithmic models. These datasets underrepresent minorities, immigrants, and peripheral communities who already face disparities in access [15].

Without systematic auditing, algorithms risk amplifying inequities — such as misclassifying high-risk patients during transport, or overlooking marginalised populations in trauma dashboards [2, 13]. No Israeli body currently mandates bias testing, leaving lifesaving decisions vulnerable to skewed data and violating the ethical principle of justice [16]. These records typically include electronic health records, triage classifications, diagnostic codes, vital signs, and documented clinical outcomes. Again, they reflect patterns of care among patients who accessed emergency services, rather than the broader population, potentially embedding pre-existing disparities into algorithmic models.

Recommendation

To mitigate risks of inequity, Israeli PHEM institutions should adopt rigorous fairness auditing protocols for all AI models prior to and throughout deployment. Key measures should include:

- *Mandatory demographic performance audits* to test whether algorithms perform equally across socio-economic, ethnic, linguistic, and geographic subgroups.
- *Transparent reporting of audit outcomes* to clinicians, regulators, and the public, ensuring accountability in addressing inequities.
- *Inclusive dataset development* that incorporates diverse patient populations, especially underrepresented groups in Israeli healthcare, in training and validation phases.
- *Continuous monitoring and recalibration* to prevent "algorithmic drift" from reinforcing disparities over time [7, 9, 10]. Algorithmic drift may occur when models trained on historical EMS or hospital data are deployed in evolving clinical or demographic contexts, such as population ageing, migration patterns, or changes in triage protocols. Without periodic re-validation, a model that initially performed equitably may gradually underperform in specific subgroups, thereby entrenching rather than mitigating existing disparities.

Such measures would help ensure that AI fulfills its promise of improving emergency care for all patients, rather than exacerbating pre-existing health inequities. In the uniquely diverse Israeli context, fairness in algorithmic performance is not only a technical requirement but also an ethical and societal imperative.

4. Liability and accountability

Ethical gap

As AI becomes embedded in Israeli PHEM, liability grows increasingly complex. Clinicians remain legally responsible, yet AI recommendations now shape triage, transport, and stabilisation [3, 12]. For example, Sheba's predictive transfer model can alert as to potential cardiac arrest, raising dilemmas: if paramedics follow the advice and harm occurs, are they solely liable? If they override it and the patient deteriorates, accountability is equally unclear [2, 4, 15].

No binding Israeli standards define responsibility among clinicians, institutions, and vendors. This ambiguity risks both over-reliance on AI as protection from blame and avoidance of AI out of fear, undermining safety and responsible use [17].

Recommendation

Israel requires explicit legal and institutional frameworks to clarify liability in AI-supported emergency care. Such frameworks should:

- *Define responsibility-sharing* among clinicians, institutions, and AI vendors when AI recommendations materially influence clinical outcomes;
- *Provide legal protection for clinicians* who act in good faith when balancing AI guidance with professional judgment;
- *Establish institutional accountability mechanisms,* ensuring that hospitals and EMS organisations remain responsible for validating, auditing, and

overseeing the AI systems they deploy [18];

- *Introduce vendor liability clauses* in contracts, obligating technology developers to assume partial responsibility for system errors or failures.

By clarifying these responsibilities, Israeli policymakers can reduce defensive clinical practices and build professional confidence in AI tools. Ultimately, liability frameworks must strike a balance: ensuring accountability without stifling innovation or eroding clinician autonomy [1, 14].

5. Institutional oversight and ethics committees

Ethical gap

Despite rapid AI deployment in Israeli PHEM, there is no dedicated institutional oversight. Hospital ethics committees review research, not real-time systems like AI triage, predictive monitoring, or trauma dashboards [3, 4]. For instance, Ichilov's trauma dashboard and Barzilai's AI despatch during *Operation Iron Swords* operated without mechanisms to evaluate fairness, bias, or transparency [5, 6].

This gap risks "ethical drift," where algorithms evolve through updates or vendor changes without accountability. For example, a vendor may introduce a software update that modifies triage prioritisation criteria or alters risk thresholds, without transparent disclosure to clinicians or institutional review. Over time, such incremental changes may shift decision-making norms in ways that affect patient access, equity, or clinician autonomy, without undergoing formal ethical scrutiny. Lacking multidisciplinary review forums, institutions without safeguards are needed to balance innovation with public trust [1, 10, 14].

Recommendation

To address this governance gap, hospitals and EMS providers should establish **dedicated AI ethics committees** tasked with ongoing oversight of AI deployment in emergency medicine. These committees should:

- *Evaluate proposals* for introducing new AI systems in pre-hospital and emergency contexts.
- *Conduct regular audits* to assess performance, fairness, and bias across diverse patient populations [13, 19].
- *Review vendor collaborations,* ensuring contractual obligations for transparency, explainability, and accountability.
- *Facilitate dialogue* between clinicians, technologists, ethicists, and patient representatives, integrating societal perspectives into institutional decision-making.

By institutionalising AI oversight, Israeli PHEM organisations could ensure that technological innovation aligns with ethical and legal standards. Moreover, such committees would provide clinicians with the reassurance that AI systems in use have been independently reviewed, thereby reinforcing both professional confidence and public trust [7, 9].

6. Public trust and engagement

Ethical gap

The rapid adoption of AI in Israeli PHEM has occurred with little public engagement. Patients whose data support models at MDA, Sheba, Ichilov, or Barzilai are rarely informed of its use or given opportunities for feedback [3,4,5,6]. This creates a widening "trust gap": while AI promises efficiency, the absence of transparency and participation risks eroding legitimacy [1,14].

The challenge is acute in Israel's diverse society, where minorities, immigrants, and peripheral communities — often sceptical of institutions — may view AI as imposed technology that commodifies their data without safeguards [8,13].

Recommendation

Building and sustaining public trust requires deliberate strategies that go beyond compliance with data-protection laws. Israeli EMS providers and hospitals should:

- *Launch public information campaigns* that explain the role, benefits, and limitations of AI in emergency medicine, emphasising transparency.
- *Engage patient advocacy groups and civil society* in policy discussions about AI deployment, ensuring diverse voices are represented [9,10].
- *Provide avenues for patient feedback,* such as surveys or forums, to capture real-world experiences and concerns with AI-supported emergency care.
- *Clarify patient rights,* including whether opting out of AI-supported protocols is possible, and under what conditions.

By embedding trust-building measures into governance structures, Israeli PHEM can foster legitimacy and public cooperation. Ultimately, societal trust is not a secondary consideration but a prerequisite for sustainable and ethically robust AI adoption in emergency medicine [2,7].

Summary of key recommendations

Six integrated steps are essential for responsible AI governance in Israeli PHEM:

1. ***AI ethics committees*** in EMS and hospitals;
2. ***Transparency and consent protocols*** for patients and families;
3. ***National data governance standards*** clarifying ownership and vendor obligations;

4. ***Bias auditing*** with demographic equity testing and reporting;
5. ***Liability frameworks*** defining shared responsibility;
6. ***Public consultation mechanisms*** involving patients, families, and civil society.

Conclusion

The rapid adoption of AI in Israel's pre-hospital emergency medicine (PHEM) illustrates both promise and risk. Current systems — triage at MDA, predictive monitoring at Sheba, trauma dashboards at Ichilov, and AI despatch at Barzilai — demonstrate potential gains in efficiency and preparedness, yet also expose major gaps: absent patient consent, fragmented data ownership, lack of bias auditing, unclear liability, and limited oversight [3,4,5,6].

Addressing these challenges requires coordinated governance. Institutions should establish ethics committees, consent protocols, and fairness audits, while regulators must clarify data governance, liability, and vendor accountability, alongside engaging with patients and the public.

The Israeli case offers lessons for other health systems: rapid AI deployment can outpace ethical and legal safeguards. Building governance frameworks in parallel with innovation is essential to ensure AI supports both clinical effectiveness and societal trust.

Notes:

[a] *Sheba Medical Center (Tel HaShomer) is Israel's largest and most advanced hospital, recognised as a global leader in medical innovation, research, and patient care. It serves as a major trauma, rehabilitation, and specialised treatment centre, integrating AI-assisted diagnostics and emergency response systems, to enhance healthcare delivery and clinical decision-making.*

[b] *Ichilov Hospital, officially known as Sourasky Medical Center, is one of Israel's largest and most advanced hospitals, located in Tel Aviv. It serves as a major trauma, emergency, and research centre across multiple specialties. Ichilov integrates AI-driven technologies in areas such as trauma assessment, diagnostics, and patient monitoring, enhancing emergency response and clinical decision-making.*

[c] *Barzilai Medical Center is a public general hospital located in Ashkelon, Israel. It serves both civilian and military populations in the southern region of the country, including during mass-casualty events and security emergencies. The hospital has been at the forefront of emergency preparedness, particularly in the context of conflict-related incidents, and has recently integrated AI-based systems to support rapid responder mobilisation and triage coordination.*

Authors: Rotem Waitzman (corresponding author — Rotemw1@gmail.com, https://orcid.org/0000-0002-7587-9086), Levinsky-Wingate Academic College, ISRAEL; **Moshe Z Abramowitz** (mosheabramowitz@yahoo.com), Peres Academic Canter, ISRAEL.

Conflict of Interest: None declared **Funding:** None

To cite: Waitzman R, Abramowitz MZ. Artificial intelligence in pre-hospital emergency medicine in Israel: Ethical and legal considerations. *Indian J Med Ethics.* 2026 Oct-Dec; 11(4) NS: 269-274. DOI: 10.20529/IJME.2026.012

Submission received: December 8, 2024

Submission accepted: November 4, 2025

Published online first: February 27, 2026

Manuscript Editor: Sunita Sheel Bandewar

Peer Reviewers: Manjulika Vaz, Nandini Kumar

Copyright and license

©*Indian Journal of Medical Ethics* 2026: Open Access and Distributed under the Creative Commons license (CC BY-NC-ND 4.0), which permits only non-commercial and non-modified sharing in any medium, provided the original author(s) and source are credited.

References

1. Floridi L, Cowls J, Beltrametti M, Chatila R, Chazerand P, Dignum V, et al. AI4People: An ethical framework for a good AI society. *Minds Mach (Dordr).* 2018 Nov 26;28(4):689-707. https://doi.org/10.1007/s11023-018-9482-5
2. Mittelstadt B, Allo P, Floridi L. Taddeo M, Wachter S. The ethics of algorithms: Mapping the debate. *Big Data Soc.* 2017;4(2):1-20. https://doi.org/10.1177/2053951716679679
3. Even D. At Sheba, we join forces for the heart. *Haaretz.* 2023 Oct 1[cited 2025 Nov 30]. Available from: https://www.haaretz.co.il/labels/health/heart2023/2023-10-01/ty-article-labels/0000018a-ea07-dfa2-a99e-ea6f2c240000
4. Ghert-Zand R. Israeli startup uses AI to help doctors image and diagnose cardiac issues in minutes. *The Times of Israel.* 2023 Jul 15 [cited 2025 Nov 30]. Available from: https://www.timesofisrael.com/sheba-startup-uses-ai-to-help-doctors-image-and-diagnose-cardiac-issues-in-minutes/
5. Pennic F. Israel's largest acute hospital deploys AI-based triage in ED. *Hit Consultant.* 2023 Jul 8 [cited 2025 Nov 30]. Available from: https://hitconsultant.net/2023/08/07/israels-largest-acute-hospital-deploys-ai-based-triage-in-ed/
6. Zafrir Y. The Cinderella of war: OmniTelcom's life-saving Drive Jump system. *The Marker.* 2023 Nov 23[cited 2025 Nov 30]. Available from: https://www.themarker.com/labels/israeli23/2023-11-23/ty-article-labels/0000018b-fbe4-d330-a9bb-fff6d96d0000
7. Biller-Andorno N, Ferrario A, Joebges S, Krones T, Massini F, Barth P, et al. AI support for ethical decision-making around resuscitation: Proceed with care. *J Med Ethics.* 2021 Mar; 48:175-83. https://doi.org/10.1136/medethics-2020-106786
8. Corrigan O. Empty ethics: The problem with informed consent. *Sociol Health Illn.* 2003 Nov 3;25(7):768-92. https://doi.org/10.1046/j.1467-9566.2003.00369.x
9. World Health Organization (WHO). *Ethics and governance of artificial intelligence for health: WHO guidance.* Geneva: WHO; 2021 Jun [cited 2025 Nov 30]. Available from: https://www.who.int/publications/i/item/9789240029200
10. UNESCO. *Recommendation on the ethics of artificial intelligence.* Paris: UNESCO; 2022[cited 2025 Nov 30]. Available from: https://unesdoc.unesco.org/ark:/48223/pf0000381137
11. Ginzborg D. Smart blanket and almost instant wound closure: Israeli technology that saves lives. *Israel Hayom.* 2024 May 5 [cited 2025 Nov 28]. Available from: https://www.israelhayom.co.il/tech/tech-news/article/15696968
12. Magen David Adom. Magen David Adom using AI to save lives. 2023 Mar 23[cited 2025 Nov 28]. Available from: https://www.mdais.org/en/news/230923
13. Binns R. Fairness in machine learning: Lessons from political philosophy. In: Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency (FAT). *Proc Mach Learn Res.* 2018 [cited 2025 Nov 23];81: 149-159. Available from: https://proceedings.mlr.press/v81/binns18a.html
14. Morley J, Machado CCV, Burr C, Cowls J, Joshi I, Taddeo M, Floridi L. The ethics of AI in health care: A mapping review. *Soc Sci Med.* 2020 Sep;22(9):e20214. https://doi.org/10.1016/j.socscimed.2020.113172
15. Gadiko A. Understanding and addressing AI hallucinations in healthcare and life sciences. *Int J Health Sci.* 2024;7(3):1-11. Available from: https://ideas.repec.org/a/bhx/ojijhs/v7y2024i3p1-11id1862.html
16. Beauchamp TL, Childress JF. *Principles of biomedical ethics.* 6th ed.

Oxford: Oxford University Press; 2009.
17. Naik N, Hameed BMZ, Shetty DK, Swain D, Shah M, Paul R, et al. Legal and ethical consideration in artificial intelligence in healthcare: Who takes responsibility? *Front Surg.* 2022 Mar 14;9: 862322. https://doi.org/10.3389/fsurg.2022.862322
18. Habli I, Lawton T, Porter Z. Artificial intelligence in health care: Accountability and safety. *Bull World Health Organ.* 2020 Apr 1;98(4): 251-6. https://doi.org/10.2471/blt.19.237487
19. Eyal G, Harel S, Glickman L. AI, equity, and healthcare disparities in Israel. *Isr J Health Policy Res.* 2022.

COMMENTARY

Cyberthanatology and digital immortality in bioethics

WALTER FONTANINI

Abstract

The simulation of the deceased through AI-based griefbots, avatars and data-driven memory tools has opened a new frontier at the intersection of technology and bioethics. This commentary examines the ethical implications of digital immortality — the replication of aspects of a person's identity beyond death — with particular attention to autonomy, narrative authorship and the integrity of grief. Drawing on philosophical traditions, clinical models of mourning and recent critiques from cyberthanatology, it analyses six ethical domains through a structured reasoning approach.

It argues that ethical remembrance should prioritise dignity over digital continuity and calls for anticipatory consent mechanisms, clearer safeguards for AI-based mourning tools and greater interdisciplinary engagement with cyberthanatology. Ultimately, it advocates a renewed commitment to death ethics in the digital age, grounded in the principle that "authenticity cannot be uploaded and dignity cannot be downloaded".

Keywords: *digital immortality, cyberthanatology, posthumous consent, AI-mediated mourning, griefbots, end-of-life ethics, bioethics of death*

Introduction: Death and identity in the age of digital simulation

The contemporary lifeworld is marked by the pervasive integration of artificial intelligence into domains once considered exclusively human. These technologies are transforming the most intimate aspects of human existence, including how we remember and interact with the dead. As a recent analysis in *Nature* by Worth observes, "Ready or not, the digital afterlife is here" [1] — a reality exemplified by the emergence of "griefbots" and "digital zombies": non-sentient artefacts that simulate conversational agency with the deceased. While often presented as compassionate tools, these simulations raise fundamental questions about dignity, here defined as narrative sovereignty: the moral right of an individual to remain the sole author of their life story and to be protected from algorithmic misrepresentation after death. As human mortality becomes intertwined with digital permanence, bioethics must reconsider the boundaries of the self in an era where the deceased are no longer silent, but are reconstructed as interactive and often commodified products.

The emerging field of *cyberthanatology* offers a way of addressing these concerns, exploring how digital technologies mediate experiences of death, dying, mourning and remembrance. Drawing on philosophy, psychology, law, computer science and bioethics, cyberthanatology examines the opportunities and risks that arise when human mortality becomes intertwined with digital permanence. What happens to the moral meaning of death when digital selves "survive"? Can a person's legacy be ethically simulated without their active involvement? Who owns the data of the deceased? Furthermore, how should society regulate the rapidly expanding digital afterlife industry, which commercialises memory, grief and identity?

This article addresses these questions through a structured ethical reflection on digital immortality in the context of end-of-life care, mourning and narrative identity, rather than presenting empirical findings. Adopting a theoretical methodology grounded in philosophical reasoning and supported by recent psychological and technological studies, it builds a normative framework based on established ethical principles, including autonomy, informed consent, authenticity, dignity, and existential insights into death and identity.

The argument is developed through a structured model of ethical reasoning, articulated across six thematic sections.

While previous studies have examined digital immortality's symbolic and psychological aspects [2], this article shifts the focus to bioethics, where questions of consent, authenticity, and dignity converge with the practical challenges of grief and remembrance. Rather than asking what digital mourning means, it asks what it demands of our moral frameworks, educational systems, and healthcare professionals, who now encounter death in the flesh and in code.

A critical caveat must be acknowledged at the outset. The normative framework proposed here operates within a tension identified by contemporary critics: we live in an age of what may be termed unimaginable and intractable AI sat-