JMSR
Journal of Medical and Surgical Research

Research Article

ISSN: 2351-8200

JMSR 2026 Vol XIII. n 1: 12..-12..

HEALTH 4.0: BALANCING TECHNOLOGICAL INNOVATION AND ETHICS THROUGH THE CYBERETHICS H4.0 FRAMEWORK

Aya Ouarhim[1,3]; Ahlam Achchar[4]; Mustapha El Bakkali[4]; Khalid Ennibi[1,2,3]; El Arbi Bouaiti[1,3]

[1] Biomedical and Epidemiology Research Unit (URBE), Center of Virology, Infectious and Tropical Diseases (CVMIT), Mohamed V Military Instruction Hospital, [2] Virology Laboratory, Center of Virology, Infectious and Tropical Diseases (CVMIT), Mohamed V Military Instruction Hospital, [3] Faculty of Medicine and Pharmacy, Mohammed V University in Rabat, [4] Exercise Physiology and Autonomic Nervous System Team (EPE-SNA), Laboratory of Physiology, Faculty of Medicine and Pharmacy, Mohammed V University in Rabat, Rabat, Morocco.

Corresponding author: Aya Ouarhim, **Affiliation:** Biomedical and Epidemiology Research Unit (URBE), Center of Virology, Infectious and Tropical Diseases (CVMIT), Mohamed V Military Instruction Hospital, Rabat, Morocco.
E-mail: aya_ouarhim@um5.ac.ma

Published *in* July 2026

Abstract

Introduction: Health 4.0, integrating artificial intelligence (AI), the Internet of Things (IoT), and big data into healthcare, offers opportunities to transform medical practice and improve patient care. However, its development raises ethical concerns involving privacy, autonomy, equity, accountability, and human oversight. **Methods:** We conducted a conceptual narrative review and ethical analysis based on peer-reviewed literature and authoritative governance documents identified through a targeted search completed on 31 December 2025. The analysis examined informed consent, data governance, cybersecurity, health equity, transparency, accountability, and human oversight. **Results:** Several interconnected ethical challenges were identified. Extensive collection and secondary use of health data may compromise privacy, autonomy, and meaningful informed consent. AI- and IoT-driven healthcare may also widen existing inequalities because of unequal access to digital infrastructure and technological resources. Increasing automation raises concerns regarding transparency and responsibility when technological systems contribute to errors or adverse outcomes. Based on these findings, we propose CyberEthics H4.0, an integrative framework encompassing cybersecurity, data governance, dynamic consent, equity, transparency, human oversight, and distributed accountability across the technology lifecycle**. Discussion:** These challenges require coordinated rather than isolated responses. Consent should become dynamic and continuous, while cybersecurity and data governance should be embedded throughout the technology lifecycle. Equitable access, digital literacy, transparency, and human oversight are essential to prevent exclusion and clarify accountability among healthcare professionals, developers, institutions, and regulators**. Conclusion**: Responsible Health 4.0 requires technological innovation to be accompanied by robust ethical governance. CyberEthics H4.0 provides a conceptual framework for integrating ethical principles throughout the technology lifecycle. Continuous ethical deliberation and adaptive regulation will be essential as digital healthcare continues to evolve.

Keywords: Ethical issues; Health 4.0; Technological tools; Informed consent; Human rights; Confidentiality.

Introduction

The era of Health 4.0, which refers to the adoption of the fourth industrial revolution in healthcare, has undergone notable changes. Technologies such as artificial intelligence (AI), the Internet of Things (IoT), robotics, blockchain and big data are changing the way healthcare services are delivered. [1-4] However, these advancements also give rise to crucial ethical concerns that require specific attention.

In this article, digital health is used as the broad umbrella covering eHealth, mobile health, telemedicine, electronic health records, and digital therapeutics. Health 4.0 denotes the wider connected ecosystem in which data, technologies, people, institutions, and governance interact. Healthcare 4.0 refers more specifically to the care-delivery layer of this ecosystem, while Industry 4.0 applied to healthcare describes the technological and organizational origins of these capabilities (Figure 1). While the ethical challenges associated with Health 4.0 are not novel and have persisted since the onset of the industrial era, technological advancements have notably intensified these concerns. Better theoretical understanding and

ethical knowledge are needed to manage these issues. Existing frameworks frequently address AI ethics, digital health, cybersecurity, privacy, or health equity separately, whereas the Health 4.0 ecosystem makes these domains interdependent [6–10]. An integrated framework that connects them to stakeholder responsibilities and lifecycle controls remains insufficiently developed. Our ethical analysis focused on four key areas: data confidentiality and security, informed consent, health inequalities, and accountability.

The evolution toward Health 4.0, a model based on agility, precision, and a holistic approach to wellness, is facilitated by the digital transformation. The focus is on genomic, microbiomic, and metabolomic personalization, revolutionizing the care methodology by placing a heightened emphasis on stability and optimizing patient outcomes. This new paradigm favors a proactive offer of care and a reimbursement system adapted to an active, on-demand lifestyle. In addition, the use of "smart factories" promotes the ability to respond efficiently and accurately to increased demand for healthcare services. [5] Nevertheless, despite these beneficial advances, one important issue remains: that of the underlying ethical issues. Ensuring the utmost safeguarding and confidentiality of patient data should always be our top priority. This approach is particularly important when handling personal and sensitive genomic, microbiomic, and metabolomic data. While digital transformation offers intriguing possibilities, it is crucial to stay watchful and consistently strive for a harmonious blend of technological progress and ethical principles. This article therefore aims to critically examine the principal ethical challenges associated with Health 4.0 and to develop CyberEthics H4.0 as an integrative conceptual framework addressing data governance, informed and dynamic consent, health equity, cybersecurity, algorithmic transparency, human oversight, and distributed accountability. The framework is presented as an author-developed synthesis requiring empirical validation, rather than as an already validated universal model.

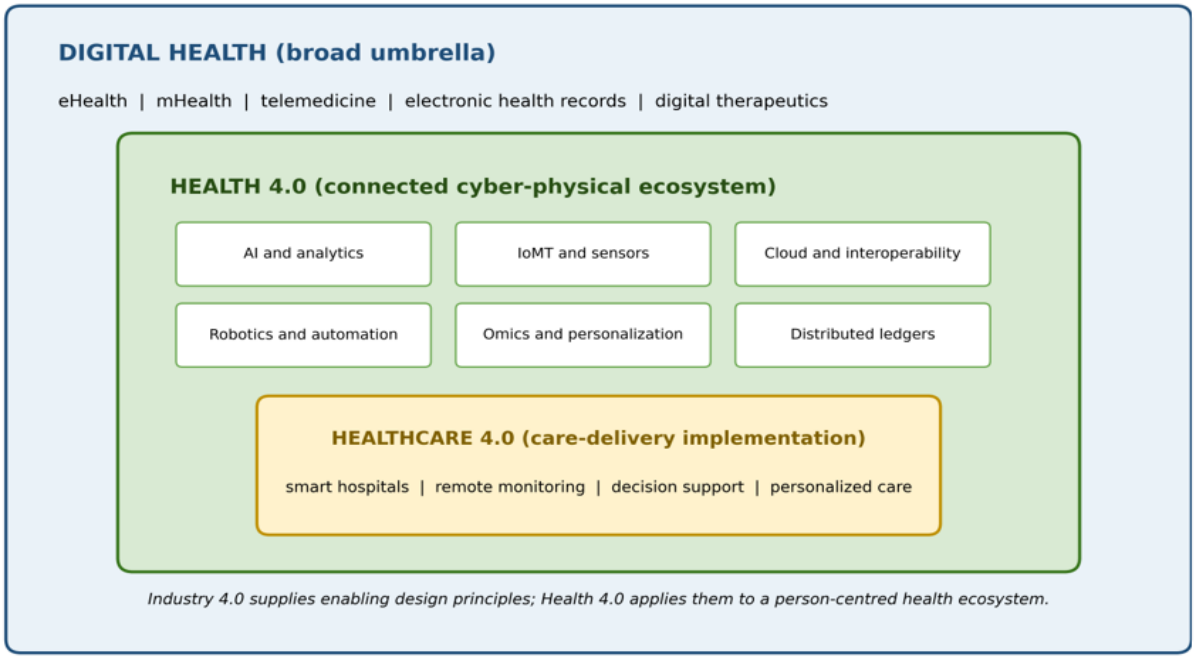

Figure 1. Conceptual relationship among digital health, Health 4.0, and Healthcare 4.0.

Methodological Approach

This article is a conceptual narrative review and ethical analysis. It does not report an empirical study and was not designed as a systematic or scoping review. A narrative approach was selected to integrate heterogeneous evidence, including empirical studies, reviews, ethical analyses, consensus guidance, and legal or regulatory documents.

A targeted literature search was conducted in PubMed/MEDLINE and in the official repositories of the World Health Organization, European Union, United Nations Educational, Scientific and Cultural Organization, United States National Institute of Standards and Technology, and United States Food and Drug Administration. The search was completed on 31 December 2025. Search concepts combined "Health 4.0," "Healthcare 4.0," or "digital health" with ethics, governance, privacy, cybersecurity, consent, dynamic consent, bias, equity, explainability, accountability, or human oversight.

Sources were included when they directly addressed Health 4.0 or a core technology used within it and analyzed ethical, governance, legal, safety, privacy, or equity implications. Priority was given to peer-reviewed literature published from January 2019 through December 2025, systematic or mapping

reviews, major medical and digital-health journals, consensus statements, and primary regulatory or international governance documents. Older sources were retained only when foundational or legally authoritative. Sources with unverifiable citation details, indirect relevance, or inadequate support for the associated claim were excluded.

The literature was synthesized thematically. First, concerns were organized around the four domains already identified in the original manuscript. Second, reviewer-requested dimensions—dynamic consent, algorithmic bias, transparency, contestability, and human oversight—were integrated. Third, the resulting domains were mapped to stakeholders and to six lifecycle stages: design, data acquisition, validation, deployment, monitoring, and retirement. Because this is a narrative conceptual analysis, no quantitative meta-analysis or formal risk-of-bias appraisal was performed.

Ethical Challenges of Health 4.0

Data confidentiality and security

Health 4.0 focuses on data privacy and security. While the collection and analysis of large amounts of data can help personalize care, they also present significant challenges for patient privacy. [11-14]

Protecting the integrity and confidentiality of patient data is essential. Healthcare data are sensitive and include family history, medical test results, and risk assessments. Thus, a wide range of security policies are required to ensure that this information is not accessible to unauthorized persons. [13]

A variety of sophisticated technological approaches are available to help protect data. Data can be stored securely with techniques such as data encryption that allow only those authorized to access it. Other methods, such as strong authentication and access rights management, also ensure that only the appropriate people can access sensitive patient information. [8,11]

Proactive monitoring systems, such as firewalls, intrusion detection systems, and physical access control measures, can significantly increase data security. This approach makes it possible to proactively identify and manage opportunities for unauthorized access or other suspicious activities. [8]

In addition, compliance with regulations is crucial for the protection of healthcare data. The General Data Protection Regulation (GDPR), for example, sets strict standards for the collection and processing of health information in Europe. [11] The European Health Data Space complements this framework with sector-specific rules for primary and secondary uses of electronic health data [12].

The ethical analysis must nevertheless move beyond the statement that data should be protected. Health 4.0 governance must specify who determines the purposes of processing, who may authorize secondary use, how data minimization and retention limits are implemented, how cross-border transfers are governed, and who is responsible when data are leaked, altered, unavailable, or reused outside reasonable expectations. The language of data stewardship is therefore preferable to treating ownership as the only relevant question.

IoT and IoMT devices broaden the attack surface because they may be resource-constrained, deployed outside controlled clinical environments, and connected to care workflows. A cybersecurity incident can therefore become a patient-safety event. Privacy-preserving approaches such as federated learning can reduce centralization, but they do not remove risks of model leakage, poisoning, unequal local data quality, or unclear responsibility across participating institutions [15].

The ethical implications are particularly evident in highly sensitive clinical domains.

Take HIV data, for example. To protect the confidentiality of people living with HIV, sensitive data such as test results, medical information and personal data must be rigorously protected. Appropriate security measures are necessary to prevent unauthorized access to this sensitive information or unintentional disclosure.

To protect the confidentiality of HIV-positive data, strict security policies and protocols must be implemented. This includes measures such as the use of firewalls, data encryption, restricted access to sensitive data and ongoing staff training on good data protection practices.

In addition, increased awareness of confidentiality and security of HIV data is needed among healthcare professionals and people living with HIV to build trust and protect personal information.

Health 4.0 development depends on data confidentiality and security. Organizations need to implement robust security policies, keep up with technological advances, and comply with applicable laws to maintain the integrity and confidentiality of patient data. [14]

Informed Consent and Dynamic Consent

Informed consent is crucial for Health 4.0. It is essential for healthcare professionals to clearly communicate the impact of Health 4.0 applications to enable patients to make well-informed decisions, considering the potentially complex nature of the technology. [7,16] A fundamental patient right is a clear understanding of the new technology and the consequences of its use for one’s health, which is guaranteed by informed consent. Patients should receive full, relevant, and comprehensive information about their treatment, including the use of Health 4.0 technology, to enable them to make informed decisions. [29]

Methods of informing patients must be clear, easy to use, and tailored to their unique abilities and needs. This includes an open and honest dialog about the potential benefits and risks of Health 4.0 applications, the use of clear and simple language, and the avoidance of overly complicated technical terms. [7,16]

In the context of Health 4.0, informed consent is essential for respecting patients' rights and ensuring appropriate care. This requires effective communication of relevant information using clear, accessible language, as well as a commitment to the transparency and integrity of the information provided.

This process consists of three key stages. First, healthcare professionals provide patients with relevant information about their treatment or medical procedure. This includes a detailed description of the benefits, risks, and potential alternatives. Next, patients are encouraged to actively participate in the decision-making process, taking into account their own goals, values, and preferences. Finally, the patient provides formal consent, either on a signed consent form or electronically. To ensure that patients make informed decisions and actively participate in their own medical care, this process emphasizes the importance of open communication and mutual understanding.

Traditional consent becomes more complex when AI systems and connected devices continuously process data. Consent to a clinical intervention must be distinguished from authorization for data processing or secondary use. A patient may understand the immediate treatment but may not anticipate future linkage, model training, profiling, transfer across institutions, or automated decision-making.

Dynamic consent can allow people to review information, express granular preferences, receive updates, and modify or withdraw choices over time [17]. However, it is not an ethical or legal panacea. Consent fatigue, interface complexity, unequal digital access, authentication burdens, and difficulty propagating withdrawal across derived datasets can undermine autonomy. Dynamic consent should therefore complement independent oversight, accessible non-digital alternatives, data minimization, and clear withdrawal rules (Figure 2).

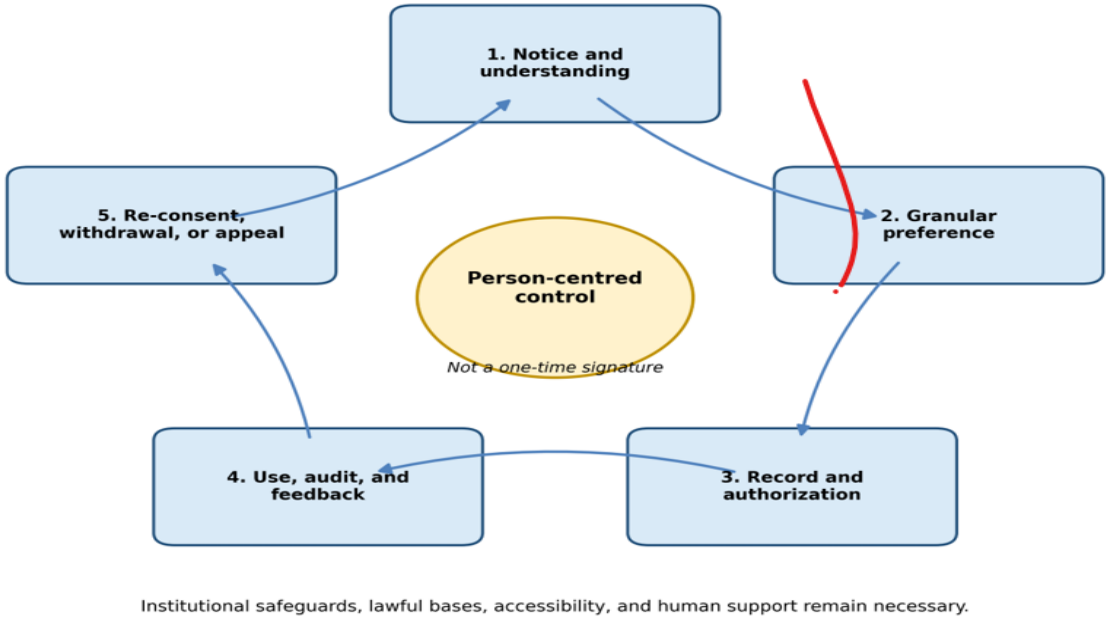

Figure 2. Dynamic consent as an ongoing, supported governance cycle.

Health Inequalities: Access and Algorithmic Inequality

Access to Health 4.0 technologies may differ significantly, potentially worsening existing health disparities. Hence, it is crucial to guarantee uniform access to these technologies. [18,19]Many factors, such as socioeconomic diversity, geographical location, age, language, health status, and digital literacy, can explain differences in access to Health 4.0 technology. If these factors are not properly addressed, they could further aggravate existing health disparities. [18,19]

Ensuring fair access to healthcare technologies is a matter of social justice that demands collaborative efforts to overcome any existing barriers. This involves putting in place measures to improve the accessibility and adoption of these technologies by everyone, regardless of their circumstances.

Methods of achieving equitable access to Health 4.0 technologies may include ensuring the availability of low-cost hardware and internet services, providing digital training for healthcare professionals, and implementing initiatives to enhance digital health literacy.

Ensuring equitable access to Health 4.0 technologies is essential for preventing the exacerbation of existing health disparities. We need to improve

accessibility and overcome the challenges that could hinder the adoption of these technologies by the most marginalized people.

Access inequality is only one pathway. Algorithmic inequality can persist even when technology is available. Models may reproduce structural inequities through non-representative datasets, biased labels, inappropriate proxy outcomes, missing data, language bias, and unequal error rates across demographic or geographic groups. Empirical studies have shown that apparently high-performing health algorithms can underestimate need or underdiagnose disease in underserved populations [20,21].

Equity assessment should therefore extend across the lifecycle. Developers and institutions should document dataset composition and intended populations, evaluate subgroup discrimination and calibration, test accessibility for older persons and persons with disabilities, monitor performance after deployment, and provide non-digital alternatives. Aggregate accuracy is not sufficient when clinically important subgroups experience disproportionate harm (Figure 3).

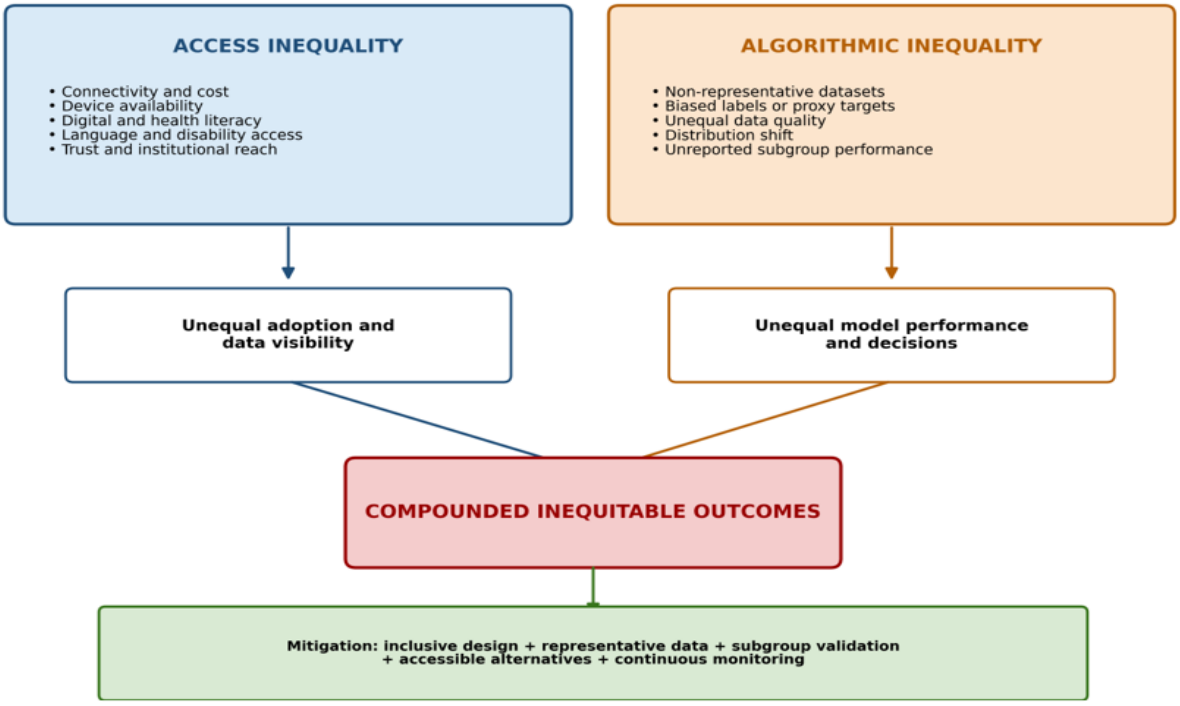

Figure 3. Dual & interacting pathways from access inequality & algorithmic inequality to unequal Health 4.0 outcome.

Transparency, Explainability, and Contestability

Transparency is broader than displaying technical model details. Patients, clinicians, institutions, auditors, and regulators require different information. Relevant disclosures include intended use, data provenance, validation population, known limitations, uncertainty, update history, human role, and routes for correction or appeal [22-24].

Explainability may support autonomy, safety, and professional judgment, but a persuasive explanation cannot compensate for an unreliable model. The useful explanation is the one that enables a specific user to act appropriately. Contestability is therefore the operational counterpart of transparency: persons affected by AI-assisted decisions should be able to request an understandable rationale, correct inaccurate data, seek human review, and challenge decisions with meaningful consequences [22,23].

Attribution of Responsibility and Human Oversight

The issue of liability in the realm of AI and robotics, especially concerning medical mistakes, can be intricate. It may therefore be necessary to establish new rules to resolve this ethical issue. [25,26]

Responsibility for medical errors involving AI and robotics can be difficult to resolve, as several actors could be involved. These actors may include AI algorithm developers, robotic device manufacturers, healthcare professionals who use the technology and healthcare institutions that provide services.

Current medical liability laws may not comprehensively address all facets of using artificial intelligence and robotics in the field of medicine. This is why new rules specifically designed for this context need to be established. These new rules could aim to clarify how to determine who is liable when AI or robotics is involved in a medical error, to what extent these actors are liable, and how to measure the impact of these technologies on patient outcomes. [25-28]

It is important to determine who is responsible for medical errors in the context of AI and robotics. To address this challenge and guarantee the ethical and safe utilization of these technologies in medicine, it might be necessary to establish new regulations.

Responsibility in Health 4.0 should be distributed but not diluted. Developers are responsible for design, data documentation, testing, and updates; manufacturers for product safety and supported maintenance; institutions for procurement, local validation, integration, staffing, and monitoring; clinicians for use within intended scope and appropriate professional judgment; and regulators for proportionate rules and post-market oversight. Table I translates this shared responsibility into minimum operational duties.

Meaningful human oversight is more than placing a clinician nominally "in the loop." The clinician must have sufficient time, authority, competence, information, and a realistic ability to question or override the system. Institutions and vendors must not transfer systemic failures to individual professionals by invoking human oversight without providing these conditions [25-27].

Table I. Minimum responsibilities for accountable Health 4.0 governance.

Actor	Minimum responsibilities	Expected evidence
Developers & manufacturers	Define intended use; document data and limitations; test safety, bias, and cybersecurity; manage updates.	Technical file, validation report, subgroup results, update and incident records.
Healthcare institutions	Perform procurement review and local validation; integrate workflows; train staff; monitor performance and incidents.	Governance approval, local test report, monitoring dashboard, escalation plan.
Healthcare professionals	Use within intended scope; explain the human role; exercise judgment; document overrides and report incidents.	Clinical documentation, competency records, incident and override logs.
Regulators & policymakers	Set risk-based requirements; coordinate data, device, cybersecurity, and liability rules; provide redress.	Regulatory decisions, audit findings, post-market actions, public guidance.
Patients & communities	Participate in design and governance; express preferences; report harms; request review or correction.	Co-design records, consent choices, complaints, appeal outcomes.

Toward a CyberEthics H4.0 Framework

With this in mind, it is timely to examine the development of an integrative framework, termed "CyberEthics H4.0," which aims to address these particular ethical challenges.

CyberEthics H4.0 focuses on the close relationship between technology, data, and healthcare, with an emphasis on the users and technologies involved. This approach recognizes the need for specific ethical responses to emerging issues in Health 4.0.

A key aspect of CyberEthics H4.0 is the recognition of cybersecurity as an essential pillar. With the increasing integration of technology and data in healthcare, it is crucial to guarantee the confidentiality, integrity, and availability of sensitive medical data. Protection against cyber-attacks and privacy breaches thus becomes a priority for preserving the trust of patients and healthcare professionals. In addition, CyberEthics H4.0 encompasses reflections on the ethical implications of using artificial intelligence, the Internet of Things, and big data in healthcare. This includes issues such as algorithmic transparency and accountability, automated decision-making, and potential biases in artificial intelligence systems. Ensuring the ethical use of these technologies requires an appropriate regulatory framework and heightened awareness of ethical issues.

In sum, the CyberEthics H4.0 concept represents an integrative approach to addressing the unique ethical challenges posed by the integration of technology, data, and healthcare in the Health 4.0 era. By focusing on users, technologies, and cybersecurity, this concept provides a solid foundation for guiding ethical decisions and promoting the responsible use of technologies in healthcare. Its contribution is not the invention of new ethical principles, but the coordination of established principles within a single Health 4.0 governance architecture.

The revised framework comprises six mutually dependent pillars:

1. autonomy and dynamic consent;
2. data stewardship, privacy, and cybersecurity;
3. equity and inclusive access;
4. transparency, explainability, and contestability;
5. clinical safety and meaningful human oversight;
6. distributed accountability and adaptive governance. The person, human dignity, and public interest remain at the centre.

Operationally, CyberEthics H4.0 follows the technology lifecycle from design and data acquisition through validation, deployment, monitoring, and retirement. At each stage, responsible actors should document risk ownership, evidence, decisions, incidents, and corrective actions. The framework is a governance overlay and does not replace professional ethics, clinical evaluation, law, quality management, or technical cybersecurity standards (Figure 4).

Figure 4. CyberEthics H4.0: an integrated, person-centred, lifecycle-based framework for Health 4.0 governance.

Comparison with Existing Ethical and AI-Governance Frameworks

CyberEthics H4.0 overlaps with established frameworks and should be positioned as complementary rather than universally superior. Biomedical principlism provides normative grounding; WHO guidance establishes globally relevant AI-for-health principles; the NIST AI Risk Management Framework provides an operational risk process; the EU AI Act establishes binding risk-based obligations; and FUTURE-AI offers healthcare-specific best practices [7–10,27–29]. CyberEthics H4.0 adds an explicit Health 4.0 ecosystem lens connecting cybersecurity, secondary data use, dynamic consent, equity, clinical oversight, stakeholder duties, and lifecycle controls.

Table II. Comparison of CyberEthics H4.0 with selected established frameworks.

Framework	Primary focus	Principal strength	Boundary or gap addressed by CyberEthics H4.0
Biomedical principlism [29]	Autonomy, beneficence, non-maleficence, justice	Normative ethical foundation	Does not itself specify technical lifecycle controls or distributed digital responsibility.
WHO AI-for-health guidance [7]	Ethical AI for health	Globally relevant principles	Centres AI; less explicit integration of IoMT cybersecurity and consent operations.
NIST AI RMF [8]	Govern, map, measure, manage AI risk	Operational risk-management process	Cross-sector framework rather than a complete health-ethics architecture.
EU AI Act [9]	Binding risk-based AI obligations	Legal duties for high-risk systems	Does not integrate every ethical concern or non-AI component of Health 4.0.
FUTURE-AI [27]	Trustworthy and deployable healthcare AI	Detailed healthcare-AI best practices	Primarily AI-focused rather than the wider connected Health 4.0 ecosystem.
CyberEthics H4.0	Integrated Health 4.0 governance	Links ethics, cybersecurity, equity, consent, oversight, actors, and lifecycle	Conceptual framework requiring stakeholder validation and implementation testing.

Discussion

The analysis shows that the principal ethical challenges of Health 4.0 are not independent checklist items. They are tensions within a sociotechnical system. Greater data access may improve model performance while increasing privacy risks; personalization may benefit some groups while excluding others; automation may improve consistency while weakening situational judgment; and transparency may support trust while creating false reassurance if the underlying model is unreliable.

The proposed framework responds to the identified gap by treating cybersecurity, consent, equity, transparency, safety, and accountability as coupled governance functions. It preserves the four ethical domains of the original manuscript while extending them to dynamic data use, algorithmic inequality, contestability, meaningful human oversight, and lifecycle governance. Its originality is therefore integrative and operational rather than based on a claim to previously unknown ethical principles.

Context remains essential. High-resource institutions may implement formal AI committees, security operations, continuous monitoring, and sophisticated consent platforms, while lower-resource settings may face connectivity, workforce, interoperability, and regulatory constraints. Proportionate implementation should prioritize high-consequence risks, accessible alternatives, shared infrastructures, open standards, and capacity building without reserving safe innovation for wealthy systems.

Practical and Policy Implications

Policymakers and regulators should connect data protection, medical-device regulation, cybersecurity, professional responsibility, and patient rights. Minimum requirements should include a clear intended use, documented data governance, independent clinical evaluation, subgroup reporting, meaningful human oversight, cyber incident reporting, post-market monitoring, and accessible redress.

Healthcare institutions should establish multidisciplinary governance before procurement. Local validation, workflow and usability testing, staff training, override and escalation procedures, monitoring thresholds, and plans for model updates or withdrawal should be documented.

Developers and manufacturers should implement representative data governance, human-factors engineering, security by design, transparent documentation, subgroup and stress testing, supported update pathways, and credible post-market surveillance. Model updates should be versioned and revalidated in proportion to their clinical impact [24,31].

Healthcare professionals require digital and AI literacy concerning intended use, uncertainty, bias, automation bias, documentation, consent, patient communication, and incident reporting. Patients and communities should participate not only through individual consent but also through co-design, governance, evaluation, and mechanisms for correction and appeal.

Limitations

This article has several limitations. It is a targeted narrative review rather than a systematic review, so source selection is vulnerable to incompleteness and interpretive judgment. The analysis prioritizes English-language literature and international or European governance documents and may underrepresent regional legal traditions and local implementation experience. The regulatory environment changes rapidly. Finally, CyberEthics H4.0 is a conceptual synthesis that has not yet undergone formal Delphi validation, prospective implementation, or evaluation against patient and organizational outcomes.

Future Research Directions

Future research should validate the framework through multidisciplinary and international stakeholder methods involving patients, clinicians, developers, ethicists, cybersecurity specialists, regulators, and representatives from low- and middle-income countries. Consensus work should determine which controls are essential across all applications and which should vary with clinical consequence, autonomy, population scale, and system adaptivity.

Measurable indicators are also required for each pillar, including consent comprehension and revocation performance, data provenance and cyber-resilience metrics, subgroup calibration and error rates, explanation usefulness, override appropriateness, incident-response time, and completeness of responsibility documentation. Research should additionally examine continuously learning models, federated infrastructures, digital twins, robotics, and generative or multimodal AI [30].

Conclusion

The Health 4.0 revolution in medical technology heralds' substantial changes in healthcare. Given the new era in which technology and healthcare are inextricably linked, there is a plethora of opportunities for substantial optimization of the quality, accuracy, and efficiency of medical services. Assigning responsibility is a difficult issue that needs to be addressed, but these potential benefits are not without ethical challenges and problems.

Who will be held responsible if a technological failure affects patients' health? To navigate this new landscape, it is essential to clarify legal and ethical responsibilities. In brief, if we truly want to benefit from the substantial advances of Health 4.0, we need to examine these ethical issues in depth. We could help shape a future in which technology improves healthcare for the greatest number while respecting the rights and dignity of each individual by protecting confidentiality, encouraging informed consent, ensuring that care is accessible to all, and establishing clear accountability. Health 4.0 should therefore be evaluated not only by technical performance but also by its effects on dignity, safety, equity, autonomy, and public trust.

CyberEthics H4.0 contributes an integrated, person-centred, and lifecycle-based architecture that connects the original ethical concerns of the manuscript to contemporary questions of cybersecurity, dynamic consent, algorithmic bias, transparency, human oversight, and distributed responsibility. The framework now requires stakeholder validation, measurable indicators, and empirical implementation studies before it can be considered operationally established.

Acknowledgements: The first author would like to dedicate this work to her daughter, Arinas, whose presence has been a constant source of strength and inspiration.

Funding: This work was supported by Centre National pour la Recherche Scientifique et Technique (CNRST), Morocco, under the 'PhD-Associate Scholarship - PASS' program [1660UM5R2023]. The funding body had no role in this manuscript's intellectual content and writing.

Conflict of Interest: The authors have no relevant financial or non-financial interests to disclose.

Ethics Approval: Not applicable. This conceptual narrative review analyzed published literature and public governance documents and involved no human participants, animals, or identifiable personal data.

Data Availability: Not applicable. No new datasets were generated or analyzed for this conceptual narrative review.

Author Contributions: All authors contributed to the study conception and the critical revision of the manuscript. All authors read and approved the final version.

References

1. Al-Jaroodi J, Mohamed N, Abukhousa E. Health 4.0: on the way to realizing the healthcare of the future. IEEE Access. 2020; 8: 211189–211210. doi:10.1109/ACCESS.2020.3038858.
2. Sony M, Antony J, Tortorella GL. Critical success factors for successful implementation of Healthcare 4.0: a literature review and future research agenda. Int J Environ Res Public Health. 2023;20(5):4669. doi:10.3390/ijerph20054669.
3. Cruz Júnior JA, Dias EM, Scoton MLD, Branco BHM. Health 4.0 in the medical sector: a narrative review. Rev Assoc Med Bras. 2024;70(1):e20231149. doi:10.1590/1806-9282.20231149.
4. World Health Organization. Global strategy on digital health 2020–2025. Geneva: World Health Organization; 2021. Available from: https://www.who.int/publications/i/item/9789240020924 . Accessed 31 Dec 2025.
5. Chute C, French T. Introducing Care 4.0: an integrated care paradigm built on Industry 4.0 capabilities. Int J Environ Res Public Health. 2019;16(12):2247. doi:10.3390/ijerph16122247.
6. 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;260: 113172. doi:10.1016/j.socscimed.2020.113172.
7. World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. Geneva: World Health Organization; 2021. Available from: https://www.who.int/publications/i/item/9789240029200 . Accessed 31 Dec 2025.
8. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg: National Institute of Standards and Technology; 2023. doi:10.6028/NIST.AI.100-1.
9. European Parliament and Council of the European Union. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Off J Eur Union. 2024;L 2024/1689. Available from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj . Accessed 31 Dec 2025.
10. United Nations Educational, Scientific and Cultural Organization. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO; 2021. Available from: https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence. Accessed 31 Dec 2025.
11. European Parliament and Council of the European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Off J Eur Union. 2016;L119:1–88. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj Accessed 31 Dec 2025.
12. European Parliament and Council of the European Union. Regulation (EU) 2025/327 on the European Health Data Space. Off J Eur Union. 2025; L 2025/327. Available from: https://eur-lex.europa.eu/eli/reg/2025/327/oj. Accessed 31 Dec 2025.
13. Zuo Z, Watson M, Budgen D, Hall R, Kennelly C, Al Moubayed N. Data anonymization for pervasive health care: systematic literature mapping study. JMIR Med Inform. 2021;9(10): e29871. doi:10.2196/29871.
14. Nittari G, Khuman R, Baldoni S, Pallotta G, Battineni G, Sirignano A, Amenta F, Ricci G. Telemedicine practice: review of the current ethical and legal challenges. Telemed J E Health. 2020;26(12):1427–1437. doi:10.1089/tmj.2019.0158.
15. Rieke N, Hancox J, Li W, Milletarì F, Roth HR, Albarqouni S, Bakas S, Galtier MN, Landman BA, Maier-Hein K, Ourselin S, Sheller M, Summers RM,

Trask A, Xu D, Baust M, Cardoso MJ. The future of digital health with federated learning. NPJ Digit Med. 2020; 3: 119. doi:10.1038/s41746-020-00323-1.
16. Aggarwal R, Farag S, Martin G, Ashrafian H, Darzi A. Patient perceptions on data sharing and applying artificial intelligence to health care data: cross-sectional survey. J Med Internet Res. 2021;23(8):e26162. doi:10.2196/26162.
17. Teare HJA, Prictor M, Kaye J. Reflections on dynamic consent in biomedical research: the story so far. Eur J Hum Genet. 2021;29(4):649–656. doi:10.1038/s41431-020-00771-z.
18. Sieck CJ, Sheon A, Ancker JS, Castek J, Callahan B, Siefer A. Digital inclusion as a social determinant of health. NPJ Digit Med. 2021;4(1):52. doi:10.1038/s41746-021-00413-8.
19. Latulippe K, Hamel C, Giroux D. Social health inequalities and eHealth: a literature review with qualitative synthesis of theoretical and empirical studies. J Med Internet Res. 2017;19(4): e136. doi:10.2196/jmir.6731.
20. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019; 366 (6464): 447–453. doi: 10.1126/science.aax2342.
21. Seyyed-Kalantari L, Zhang H, McDermott MBA, Chen IY, Ghassemi M. Underdiagnosis bias of artificial intelligence algorithms applied to chest radiographs in under-served patient populations. Nat Med. 2021;27(12):2176–2182. doi:10.1038/s41591-021-01595-0.
22. Amann J, Blasimme A, Vayena E, Frey D, Madai VI. Explainability for artificial intelligence in healthcare: a multidisciplinary perspective. BMC Med Inform Decis Mak. 2020;20(1):310. doi:10.1186/s12911-020-01332-6.
23. Ghassemi M, Oakden-Rayner L, Beam AL. The false hope of current approaches to explainable artificial intelligence in health care. Lancet Digit Health. 2021;3(11):e745–e750. doi:10.1016/S2589-7500(21)00208-9.
24. US Food and Drug Administration, Health Canada, Medicines and Healthcare products Regulatory Agency. Transparency for machine learning-enabled medical devices: guiding principles. 2024. Available from: https://www.fda.gov/medical-devices/software-medical-device-samd/transparency-machine-learning-enabled-medical-devices-guiding-principles . Accessed 31 Dec 2025.
25. Habli I, Lawton T, Porter Z. Artificial intelligence in health care: accountability and safety. Bull World Health Organ. 2020;98(4):251–256. doi:10.2471/BLT.19.237487.
26. Reddy S, Allan S, Coghlan S, Cooper P. A governance model for the application of AI in health care. J Am Med Inform Assoc. 2020;27(3):491–497. doi:10.1093/jamia/ocz192.
27. Lekadir K, Feragen A, Fofanah AJ, Frangi AF, Buyx A, Emelie A, Lara A, Porras AR, Chan AW, Navarro A, Glocker B, Botwe BO, Khanal B, Beger B, Wu CC, Cintas C, Langlotz CP, Rueckert D, Mzurikwao D, Fotiadis DI, et al. FUTURE-AI: international consensus guideline for trustworthy and deployable artificial intelligence in healthcare. BMJ. 2025; 388: e081554. doi:10.1136/bmj-2024-081554.
28. Siala H, Wang Y. Shifting artificial intelligence to be responsible in healthcare: a systematic review. Soc Sci Med. 2022; 296: 114782. doi: 10.1016/j.socscimed.2022.114782.
29. Beauchamp TL, Childress JF. Principles of biomedical ethics. 8th ed. New York: Oxford University Press; 2019.
30. World Health Organization. Ethics and governance of artificial intelligence for health: guidance on large multi-modal models. Geneva: World Health Organization; 2024. Available from: https://www.who.int/publications/i/item/9789240084759 . Accessed 31 Dec 2025.
31. International Medical Device Regulators Forum. Machine learning-enabled medical devices: key terms and definitions and Good Machine Learning Practice principles. 2025. Available from: https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-device-development-guiding-principles . Accessed 31 Dec 2025.