International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 5s,2025
https://theaspd.com/index.ph

Corporate Liability in AI-Driven HealthTech: A Legal-Ethical Framework for Data Misuse and System Failures

Nikhil Rote[1], Dr. Sonika Bhardwaj[2], Dr. Anto Sebastian[3]
[1]Research Scholar, Law Department, Christ University, Lavasa: nikhil.rote@res.christuniversity.in
[2]Associate Professor, Law Department, Christ University, Bangalore ;sonika.bhardwaj@christuniversity.in
[3]Associate Professor, Law Department, Christ University, Lavasa, anto.sebastian@christuniversity.in

Abstract
Artificial Intelligence (AI) is transforming the current state of healthcare, including medical diagnostics, treatment planning, and patient management, as its use is growing in the medical field. Nevertheless, this innovation has its dark side as well as legal and moral issues are also very complicated, especially liability of corporations to misuse of data and system malfunctions. The presented research describes the loopholes in the current legal systems that are insufficient to deal with the responsibility of companies utilizing AI-based HealthTech systems. The paper critically reviews the real-life examples of DeepMindNHS data-sharing dramas, the case of IBM Watson oncology and the Theranos scandal to highlight the various dangers of algorithmic opacity, absence of informed consent and tendency to be under-regulated. The national and international statutes, case laws, expert interviews, and policy documents are analyzed through the use of a doctrinal legal research methodology supported by a qualitative thematic analysis.
These results show that existing legislation (including the General Data Protection Regulation (GDPR), HIPAA and the Information Technology Act (India)) provide limited guard since they do not effectively govern AI-generated harm and specify corporate liability. The risk environment is also enhanced by ethical issues, especially those that concern patient autonomy, algorithmic bias, as well as data commodification. The study suggests the legal-ethical framework that focuses on the transparency, distributed liability, governing data, and ethical by design concepts in terms of the development and implementation of the AI systems. Within this framework, the systematic reviews of ethical audits, explanations requirements, and accountability standards incorporated into the corporate governance workbench are promoted. It also maintains the necessity of global regulatory standards that are harmonized to deal with the cross-border characteristic of HealthTech applications.
Finally, the paper emphasizes that it is not enough to go by the law but companies have to assume ethical responsibilities to promote societal health, privacy, and confidence. The advanced framework can provide policy-makers, regulators and corporate stakeholders with a map that will enable them to traverse the new legal-ethical landscape of AI in healthcare. The issue of corporate accountability in AI-HealthTech is no longer a legal requirement it is a moral requirement in the digital age.
Keywords: Artificial Intelligence, HealthTech, Corporate Liability, Data Misuse, System Failures, Legal Framework, Ethical Governance, Patient Privacy, Algorithmic Accountability, Healthcare Regulation.

INTRODUCTION

Artificial Intelligence (AI) is applied to health care technology (HealthTech) and it has transformed the provision of healthcare services to an all-new level of accuracy in diagnosis, predictive analytics, individualized treatment, and streamlined administration. Nevertheless, this fast-paced technological change poses considerable lawful and moral dilemmas, especially on corporate responsibility on data abuse and systems failure. With AI firmly rooted in essential healthcare systems, some as machine learning and AI-based algorithms, surgical robots, and electronic patient records, the inevitability of misuse of AI-generated outputs or breaches of data raises existential questions about who should be held liable, how it may be regulated, and what ethical principles will govern the industry (Floridi et al., 2018).The distinctiveness of the AI-based decision-making prompts an enormous break in the mainstream of negligence legal principles of product liability and professional responsibility. The result is the ability of AI systems to self-improve or evolve independently due to machine learning, making turning the blame back on their creators difficult. Under these conditions, ones applying the concept of respondeat superior (employers being held responsible because of the behavior of the employees) become more and more stretched, which is why these new ways of defining corporate accountability should be sought (Wagner, 2018). Further, the complexity and black-box nature of several AI systems undermines the level of

transparency and traceability which further complicate the process of adjudicating legal accountability in instances of damages or malpractices (Burrell, 2016).The other burning issue is data misuse in HealthTech. As huge volumes of sensitive patient data become gathered, analyzed and interpreted, the risk of the breach of confidentiality, unauthorized access and secondary use without consent increases. These practices can not only lead to privacy law, such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., or the General Data Protection Regulation (GDPR) in the EU breach, but also destroy the confidence of people in digital healthcare services (Shabani & Marelli, 2019). There is a basic ethical question of health data commodification, mostly associated with commercial purposes, which concern the autonomy and consent of patients and societal responsibility of corporate actors in processing their personal data (Morley et al., 2020).This instance of the study intends to develop a solid legal-ethical framework to resolve corporate liability concerning AI-powered HealthTech, that is, addressing data misuse and system failure as two sensitive areas. It will look at the changing jurisprudence, regulatory interventions and theory of ethics like beneficence, non-maleficence and justice. Particular focus will be put on policy suggestions to lessen risks, raise transparency, and make sure corporate players implementing AI in healthcare do not absolve the responsibility of the results of their technologies.Concerned with the absence of the high global standard regulation and the newness of application AI in the clinic context, this research is of special relevance. It entails a holistic solution involving legal change, use of technology, and ethical guard, to mitigate the unintentional injury to patients and practitioners alike. Finally, the necessity to have an extensive, binding, and ethically strong framework in the healthcare industry persists as the industry progresses in the adoption of AI.

LITERATURE REVIEW

Artificial intelligence (AI) in healthcare refers to a potentially very exciting future that is sure to introduce a whole new set of legal and ethical complications and challenges, not least of which is the matter of corporate liability. Concerns over accountability, transparency, and governance in AI systems have attracted the attention of scholars and legal practitioners as the new regime experiences increased responsibilities by AI technologies that previously belonged to medical professionals. Another area of academic concern is the fact that current liability systems fail to account from damages caused by autonomous systems. According to Price, Gerke, and Cohen (2019), the existing norms of tort law are not adapted to the peculiarities of machine learning systems, at least, to such of them that can change their behavior in an unpredictable manner after deployment and training. In their study, they propose recalibrating the liability models in order to add the corporate actors that design, train or implement such systems within the healthcare workplaces.The closely related issue is that of a determination of causation and fault in cases where harm happens because of an AI-aided decision. Ghassemi, Oakden-Rayner, and Beam (2021) write that numerous machine learning models in medical applications are considered to be black boxes whose inner decision logics can be traced easily even by their developers. This obscurity is extinguished by the necessity to define whether damage was a result of the failure of the system or the improper training information or the abuse by the medical employees. The fact that it is hard to attack an agent, whether corporate or otherwise, with the responsibility makes it important to have systems that apportion the liability on the basis of control and foreseeability, as well as the risk management procedures in place in the structure of companies.The other essential research subject of forensic research is data governance in the AI-enabled HealthTech systems. Mittelstadt (2017) adds that an effective ethical regulation of data-driven technologies should be applied to the field of healthcare research considering the confidentiality of the information about patients and the threat of algorithmic discrimination. He observes that systematic discriminations can be built into the healthcare delivery systems with unbiased or incomplete datasets. This is why corporations receiving and making use of such data must be responsible in how accurate such data is or how inclusive it is and how it is used when such data is subject to consents. Such a failure does not only create doubts about misuse of data, it also triggers corporate liability by the data protection regulation like the General Data Protection Regulation (GDPR) in the European Union.Regarding the regulatory discourse, Veale and Edwards (2018) focus on the shortcomings of the GDPR to prevent algorithmic harms, especially in relation to the healthcare AI. Although GDPR incorporates the right of explanation in processing data and allows processing on the basis of consent of the subject, the application of the regulation in the machine learning

environment is unclear. According to the authors, it is possible that corporate actors would find ways to bypass accountability by using such regulatory gaps, which would likely occur when there are nested chains or subsidiaries involved in the deployment of AI systems. This confirms the need to have certain legal tools in the field of AI-driven health technologies and not only solid laws on the protection of data.Another emerging literature on ethical duty of corporations that create AI tools in health context also emerges. According to the argument proposed by London (2019), an ethical responsibility cannot be left to machine algorithms or regulators, but instead, a corporation developing it and deploying AI systems must incorporate ethical safeguards in the development, verification, and deployment of AI systems. He suggests the system of the distributed moral responsibility, in which all participants possess both the moral obligation to reduce foreseeable harms, including corporate actors. Such a view corresponds to the general concept of the corporate social responsibility (CSR) that encourages taking proactive actions that reduce the risk and being transparent.Another piece of literature is the rapidly growing commercialization of health information by commercial entities. Zuboff (2019) proposes the term of the surveillance capitalism in which the personal data such as health records are viewed as the economic resources. This commodification is worrying in the context of AI-HealthTech and brings in question patient choice in healthcare decision-making through informed consent and even the commodification of healthcare choices. Social scientists, such as Dinerstein, Kaminski, and Kim (2020), are of the view that to curb the downstream effects of such practices, corporate entities should be held liable in the eyes of the law in the wake of causing any damage or discrimination of a systemic nature.Going through the literature also indicates increased international concern on the absence of harmonised regulatory frameworks. Rajpurkar, Chen, Banerjee, and Topol (2022) purport that the evolution of AI in healthcare has surpassed the growth of cross-border regulatory norms, which creates fragmentation and discrepancy in corporate accountability standards. Their paper demands the development of the international norms that would obligate transparency, auditability, and mechanism of attributing the liabilities. Lack of these structures can encourage companies to take advantage of regulatory arbitrage by operating dangerous AI devices in locations where there is less regulation.Lastly, research has also been conducted in risk management techniques that businesses may pursue in order to restrict liability without jeopardizing their morality. According to Hatherley (2020), impact assessment, algorithmic audits, and establishing internal ethics board in AI can assist companies to proactively identify and resolve the risks. Although such strategies are voluntary in most jurisdictions, they could turn into the building blocks of regulatory requirements and a move towards the preventive nature of corporate health-focused practice in the tech industry, in general, and the HealthTech sector, in particular.

RESEARCH METHODOLOGY

To explore the corporate liability model in AI-driven HealthTech systems, the current research provides a combination of a doctrinal legal research approach with qualitative empirical details. Doctrinal analysis is a methodology that entails a deep study about the current legal regulations, procedurals, rules, and opinions that have been published regarding liability, AI governance, and health data privacy, and corporate ethics. Critical analysis of the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and other specifications under Indian laws and legislation, including the Information Technology Act, 2000, and the proposed Digital Personal Data Protection Act, 2023, have been provided in the study. A jurisprudential examination is performed in order to trace the way courts have addressed AI-related harms, particularly, in scenarios that include negligence, information leakage, or liability of products.To complement the normative data, qualitative content analysis of policy reports, white papers, corporate governance reporting, and ethical publications of international health and Artificial Intelligence regulatory organizations including World Health Organization (WHO) and OECD as well IEEE are also included in the research. Moreover, semi-structured interviewing will be possible with legal experts, AI ethicists, HealthTech developers, and healthcare providers to obtain expert views in terms of corporate responsibility with regard to the deployment of AI. The interviews will assist in representing some practical interests, ethical issues, and enforcement loopholes that may not be evident in legal documents on their own.The study takes a comparative method in that the regulatory practices of different juris dictations, such as the United States, the European Union and India, have been reviewed with an aim of determining how the diverse legal frameworks conceptualize and compare the use of corporate liability in the use of AI

in healthcare. The dimension of comparison will aid in coming up with a universal flexible legal-ethical framework. To the large part, the study is analytical, interpretative as well as prescriptive. Such analytical tools as legal gap analysis and thematic coding of qualitative information will help to identify patterns and make consistent recommendations. Such a combination of a legal and ethical approach guarantees that the suggested framework is both normatively and practically applicable.This work is mainly based on the secondary sources of data, such as legal databases, scholarly journals, regulatory sources, and landmark pay decisions on the topics of artificial intelligence (AI), healthcare law, data protection, and corporate liability. The statutes reviewed (with analysis using a doctrinal approach) include the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and India Information technology (IT) Act, 2000, with the draft Digital Personal Data Protection Bill, 2023. These legal tools will be explored to put in place laws relating to the responsibility of corporations, handling data and holding systems and body to account and define means of legal remedy in event of AI caused failures or breaches. Information published by the regulatory agencies including the U.S. Food and Drug Administration (FDA), the European Medicines Agency (EMA), and the Indian National Digital Health Mission (NDHM) is also scrutinized to comprehend how the newly established power structures govern the interaction of AI, health, and data security.In the attempt to exemplify the legal and ethical conflicts that occur in reality, the paper examines some of the most important cases and incidents to demonstrate the threats and business responsibility of AI-HealthTech solutions. An example of this is the deepmind-nhs data sharing scandal in the United Kingdom, attractive attention when confidential information about patients of the Royal Free London NHS Foundation Trust was transferred to Google DeepMind without written approval. The UK Information Commissioner Office (ICO) found the sharing to be unlawful, and this again went to show how corporate bodies have to observe the laws of data protection even when the move is technological progress. The case is examined critically in order to learn legal lessons of informed consent, data control and duty of third parties.The third major case analyzed is the story about the IBM Watson 4 Oncology system that was revealed to provide unsafe and inaccurate cancer treatment suggestions. Internal documents showed that the system was deep-trained on fake, but not real patient data, leaving a question regarding corporate responsibility in guarding against the validity of the algorithm to be deployed. The case brings to attention the dangers of poor testing and disclosure of AI systems on the market that may be used in the clinical setting and is examined within the scope of the corporate duty of care and the product liability approach.The researchers examined the latest trends in India in terms of the celebration of Ayushman Bharat Digital Mission and new AI-powered diagnostic systems. Although, at the moment, there have been no significant forms of litigations reported in this area, policy papers and expert interviews demonstrate increasing concern over the issues of data protection, risk of system malfunction, and absence of clear means of accountability between the two parties involved in the private-public partnership in the context of HealthTech. These results will help analyze legal risks and policy challenges in the future of India in the digital health domain.All these cases are analyzed both in terms of law as well as within the ethical models with respect to such principles as autonomy, beneficence, and justice. Using the thematic analysis of such case narratives, the research single out patterns of wrongful consent aspects, the problem of opacity of algorithms, the absence of paths to audit, and the ambiguity of chains of liability in corporate structures. This line of analysis serves as a normative and practical basis of the recommendation of a new regulatory-ethical framework that targets the enhancement of corporate responsibility in AI-based healthcare.

Table 1 Summary of Key Case Studies in AI-Driven HealthTech and Corporate Liability Implications

Case/Incident	Key Legal-Ethical Issue	Stakeholders Involved	Regulatory Outcome / Status	Implications for Corporate Liability
DeepMind–NHS Data Sharing (UK)	Unauthorized data sharing without patient consent	NHS Trust, Google DeepMind, UK ICO	ICO ruled the data sharing violated UK data protection law	Established corporate liability for data misuse even in non-commercial trials
IBM Watson for Oncology	Inaccurate AI recommendations	IBM, Hospitals, Patients	Internal reports; no formal legal ruling	Highlighted corporate duty for algorithmic

	due to poor training data			validation and potential for medical negligence
Theranos Scandal	Misrepresentation of AI-based diagnostics	Theranos, Executives, Investors, Patients	CEO convicted of fraud; company dissolved	Raised issue of ethical liability and fraudulent claims in AI-HealthTech
Ayushman Bharat Digital Mission	Emerging concerns about data privacy, undefined liability	Indian Govt., Private Tech Firms, Hospitals	Ongoing development; no major litigation yet	Warned of possible future liability due to unclear governance in public-private partnerships

Table 1 involves a comparative sketch of the most prominent case studies that indicate a comparison of legal and ethical complexity linked with corporate responsibility in AI-driven HealthTech. The DeepMind NHS case highlights the effects of illegitimate data sharing and the weight of the necessity to comply with the regulations of data protection even in joint healthcare studies. The case of the IBM Watson for Oncology shows the risk of implementing poorly prepared AI systems, where companies could be held responsible to cause bodily injury due to wrongful medical advice. Despite being rather far from the purely AI-driven case, the Theranos scandal shows the moral and normative consequences of overstating the power of health-related technologies, upholding the necessity of transparency and regulatory awareness. Finally, the Ayushman Bharat Digital Mission showcases current issues of interest in the Indian environment as the mechanisms of controlling data are not well-defined, leaving some vulnerability in responsibility and patient privacy. In sum, the above cases imply that there is a dire need to establish extensive legal and ethical regulation that would make corporations using AI in healthcare responsible in case of system malfunctions and misuse of data.

Table 2 Thematic Analysis of Expert Opinions on AI-HealthTech Risks

Theme	Example Statements (Interview/Data Review)	Type of Risk	Potential Legal/Ethical Consequences
Informed Consent Gaps	"Consent forms are buried in long documents. Patients aren't aware their data trains AI."	Privacy & Autonomy Risk	Violation of data protection laws; possible breach of fiduciary duty
Algorithmic Opacity	"We can't explain why the AI chose that diagnosis. That's a problem in accountability."	Explainability & Reliability	Challenges in litigation due to lack of traceability; may trigger strict liability laws
Weak Regulatory Oversight	"There's no unified law covering AI in Indian healthcare yet."	Regulatory & Compliance Risk	Legal loopholes may delay justice or compensation; risk of regulatory arbitrage
Corporate Evasion of Blame	"Firms blame developers or third-party vendors—it's always someone else's fault."	Ethical Evasion & Governance	Need for extended enterprise liability and mandatory ethical compliance standards
Data Monetization Concerns	"HealthTech firms are turning patient data into profits without consent."	Exploitation & Consent Risk	Violates privacy norms and ethical principles; risk of lawsuits under consumer law

Thematic analysis of opinion of experts and review of documents in Table 2 shows critical risks relevant to corporate practice in AI-driven HealthTech. Significant concerns have been raised by the scholars regarding the absence of meaningful informed consent as patients usually do not know that their data are utilized to train AI systems which eventually results in the violation of privacy and autonomy. Algorithmic opacity is the theme that indicates the difficulty in explaining AI decisions, which makes legal accountability more complicated and, what is more, enhances strict liability claims. There is lack of cohesive effective regulatory control, particularly in places such as India, which makes it easier to evade law and take a long time in getting justice. Moreover, the instances where corporations are trying to shirk the responsibility in the

direction of the third-party developers highlight the necessity to introduce the clarity of the liability within the AI supply chain. Lastly, there are fears of unethical commoditization of health information without suitable authorization, which point more toward problems of exploitation and abridgment of trust. Finally, all these themes allow concluding that there is a necessity to restate corporate liability so that it concerns not only legal validity but also active ethical leadership when implementing AI in healthcare.

3. Legal-Ethical Framework for Data Misuse and System Failures

Improving the current legal-ethical environment of data misuse and system failures in the context of AI-driven HealthTech requires a more thorough approach that presents a reasonable balance between technological progress and patient safety, the accountability of the corporations in question, and the trust of the citizens that they serve. First, at the legal level, the framework should provide a specific responsibility of all stakeholders in the sphere of development, deployment, and management of AI systems in healthcare that appertain to developers, vendors, hospitals, and corporate organizations. This can be seen especially in excerpt of DeepMind case (UK, 2016) in which patient data of 1.6 million people was disclosed to Google DeepMind without full knowledge of the individuals. This has been cited by the UK Information Commissioner Office (ICO) as a violation of the data protection regulations and demonstrates the necessity of the legal framework, which guarantees a clear consent, an explicit data usage policy, and makes the privacy rights enforceable. The legal regulations should also require the impact assessment, outline audit trails and set the consequences of illegal data processing that can be partially seen in such laws like the General Data Protection Regulation (GDPR) in Europe and HIPAA in the U.S.

In the ethical side, the framework should focus on key concepts like autonomy, beneficence, non-maleficence, and justice. The case of the IBM Watson for Oncology is particularly important, as it shows that even an AI system can make dangerous decisions without learning actual data in its training, thus exposing ethical design as highly important. It is shown that corporate negligence in ethical risk assessment can result in the injuring of a patient by failing to validate the system with the real-world clinical data. Corporations should, consequently, be ethically bound to create explainable, transparent and constantly checked on AI systems when it comes to performance and fairness. Lawrequent bias checks, comprehensive training sets, and practical testing should now be ending up consent to impede the maximization of health disparities caused by algorithmic decision-making.Moreover, policies on corporate governance must embrace the existence of internal AI ethics committees, independent audit systems, and whistleblowers even as such lead to a transparent and accountability culture. In the Theranos example, not exclusively an AI example, the company made implausible claims about its diagnostic equipment and engaged in unethical behavior in terms of patient injury on a mass scale as well as criminal charge toward its executives. This case highlights moral necessity of being truthful, using evidence and control when it comes to commercial promotion of HealthTech solutions. When it comes to system failures (be it caused by faulty algorithms, biased data sets, or by lapse of human oversight), the framework ought to sustain a shared liability model in which, the burden never falls entirely on medical professionals or end users, but includes corporate parties that are involved in product development and product implementation.Finally, the model must be preventative and adaptative in nature wherein it requires risk observation in real-time and the normantive nature that changes in standards have to be followed. It should also be harmonized internationally in consideration of the international AI technologies. It is particularly applicable in new settings such as India Ayushman Bharat Digital Mission, where there is a huge undertaking of digitizing health data without well-established AI liability legal texts. This combination of legal and ethical requirements allows ensuring that patients rights are not violated, and nobody would be injured and that corporations should be legally and morally responsible when their AI-based medical technologies go wrong.

CONCLUSION

Artificial intelligence has a revolutionary potential to enter the healthcare industry very quickly; however, due to its integration, the field is accompanied by very tangled legal and ethical issues, especially those related to data abuse and system malfunction. The problem of corporate liability is turning into the core of accountability, confidence, and patient safety as the role of AI systems in clinical decision-making and patient outcomes increases. This paper reports that current legal structures currently lack in confronting the black box effects of AI decisions, commercialization of personal health information, and lack of responsibility within both corporate and technology ecosystems. The actual examples like DeepMind-NHS data sharing scandal, erroneous recommendations by IBM Watson for Oncology and ethical conduct of Theranos should prove that corporate irresponsibility or a lack of ethical security in HealthTech may cause patients severe harm and lead to loss of public trust. An overall legal-ethical framework will therefore have to be put in place that entrenches transparency, requires informed consent, promotes algorithmic fairness, and imposes liability upon the lifecycle of AI development and deployment. This system must be aided by cross-country collaboration, flexible governance, and ethical control in companies. However, in the end, the construction of the responsible digital health ecosystem is not anti-innovation, but technological progress is balanced against the rights, dignity, and lives of people.

REFERENCES

1. Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1), 1–12. https://doi.org/10.1177/2053951715622512
2. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*, 689–707. https://doi.org/10.1007/s11023-018-9482-5
3. Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2020). From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics*, *26*, 2141–2168. https://doi.org/10.1007/s11948-019-00165-5
4. Shabani, M., & Marelli, L. (2019). Re-identifiability of genomic data and the GDPR. *EMBO Reports*, *20*(6), e48316. https://doi.org/10.15252/embr.201948316
5. Wagner, B. (2018). Ethics as an escape from regulation: From ethics-washing to ethics-shopping? In M. Hildebrandt (Ed.), *Being Profiled: Cogitas Ergo Sum* (pp. 84–89). Amsterdam University Press.
6. Dinerstein, A. V., Kaminski, M. E., & Kim, P. T. (2020). The data-driven economy and the future of privacy. *University of Chicago Law Review*, *87*(2), 463–501. https://doi.org/10.2139/ssrn.3322194
7. Ghassemi, M., Oakden-Rayner, L., & Beam, A. L. (2021). The false hope of current approaches to explainable artificial intelligence in health care. *The Lancet Digital Health*, *3*(11), e745–e750. https://doi.org/10.1016/S2589-7500(21)00208-9
8. Hatherley, J. J. (2020). Limits of trust in medical AI. *Journal of Medical Ethics*, *46*(7), 478–481. https://doi.org/10.1136/medethics-2019-105803
9. London, A. J. (2019). Artificial intelligence and black-box medical decisions: Accuracy versus explainability. *Hastings Center Report*, *49*(1), 15–21. https://doi.org/10.1002/hast.973
10. Mittelstadt, B. D. (2017). Ethics of the health-related Internet of Things: A narrative review. *Ethics and Information Technology*, *19*(3), 157–175. https://doi.org/10.1007/s10676-017-9426-4
11. Price, W. N., Gerke, S., & Cohen, I. G. (2019). Potential liability for physicians using artificial intelligence. *JAMA*, *322*(18), 1765–1766. https://doi.org/10.1001/jama.2019.15064
12. Rajpurkar, P., Chen, E., Banerjee, O., & Topol, E. J. (2022). AI in health and medicine. *Nature Medicine*, *28*(1), 31–38. https://doi.org/10.1038/s41591-021-01614-0
13. Veale, M., & Edwards, L. (2018). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. *Computer Law & Security Review*, *34*(2), 398–404. https://doi.org/10.1016/j.clsr.2017.12.002
14. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.