



MAY 2022

# THE ETHICS OF HEALTHCARE AI

Authored By:  
Joyce Hunter, Executive Director, ICIT  
Drew Spaniel, Lead Researcher, ICIT

---

## **The Ethics of Healthcare AI**

**May 2022**

---

Copyright 2022, The Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the [www.icitech.org](http://www.icitech.org) website, and (3) other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute.

## Contents

Introduction – How are Ethics Related to AI? .....	4
Who is Asking? .....	4
How and for whom do we define Ethics? .....	4
Whose Ethics are Defining AI? .....	5
Without Intelligent and Intentional Architecture and Design, Big Data Leads to Inequity .....	6
Separating the Science from the Fiction .....	7
Equitable Healthcare AI Depends on Education as Much as Technology .....	7
An Multi-stakeholder Healthcare AI Ethics Framework Can Reduce Inherent Biases .....	8
AI Must be Open and Accessible .....	8
Blockchain Promises to Make Data More Coherent and Understandable .....	9
Communication is Key to Understanding Limits and Goals.....	10
Stakeholders Each Have a Role and Responsibilities in the Ethical Development of AI .....	10
Conclusion - AI Promises Progress, But It Is Not a Panacea .....	10
Resources.....	11

## Introduction – How are Ethics Related to AI?

Artificial Intelligence has the potential to reshape critical infrastructure operations and security. In the healthcare sector, it is projected to significantly improve quality of life, provided it is developed with security controls, such as blockchain and security and privacy – principles, tenets, and ethics in mind. Ultimately, AI is not a silver bullet or panacea; it is a tool that we must train the rising generations to better develop, understand, and use. However, like any tool, the potential benefits of AI are inhibited by the potential for aberrant use. AI systems and machine learning algorithms are only as reliable and accurate as the data we provide and only as ethical as the constraints incorporated into the developed code. It may be incumbent upon us all to develop frameworks that increase transparency, incentivize collaboration, incorporate ethics, require privacy protections, and mandate security controls. When approaching the ethics of AI, I think it is important that we address three understated, but essential questions:

- Who is asking?
- How and for Whom do we define ethics?
- Whose Ethics are Defining AI?

### Who is Asking?

There is interest from both the public and private sector in developing artificial intelligence algorithms for healthcare applications. According to Forbes, the total public and private sector investment in healthcare AI is expected to reach \$6.6 billion in 2021. Even more promising, Accenture predicts that AI applications may result in annual savings of \$150 billion by 2026. We need to determine which stakeholder community is driving and benefitting from development and whether ethics are incorporated throughout their design lifecycle.

### How and for whom do we define Ethics?

Healthcare is a broad field that amasses more data than almost any other sector. Leveraging machine learning on healthcare data sets could reduce costs, maximize profits, or improve patient care. As a community, if we are going to develop a governing framework, we need to be clear on our goal when incorporating AI into healthcare and we need to identify and include every security and privacy control possible. After all, in every field, AI is considered because it promises the capability to more efficiently and optimally achieve a goal. Thus, it requires us to be crystal clear in our understanding and definition of that goal. I know it's early, but let's begin this morning with a difficult query; which outcome is driving healthcare AI development the most? Can we achieve every outcome? Possibly, but the other outcomes may be realized to a lesser extent, because only one outcome can be maximized. Each member of the audience may already have a different answer. Let's complicate the hypothetical. Will organizations try to maximize the quality, availability, and efficacy of care without a governing framework? Unlikely. Speaking objectively, unfettered capitalism is inherently amoral. It isn't good or bad, but it also isn't driven by ethics. Innovators could develop healthcare AI applications altruistically, but then imitators would likely disrupt the market and supplant the altruistic developers.

The central problem with ethics and healthcare in America is that at the moment, they are in conflict. Our system is set up to achieve profit, rather than maximizing health. To be clear, the conflict between the prioritization of profit over care preexists AI and the struggle will continue regardless of AI adoption. The challenge that we face is that AI is a tool that if leveraged incorrectly or amorally, could exacerbate



that dichotomy. As a result, patients may be profiled or have their data exposed without their consent, or just receive economically efficient, but ultimately inferior care.

Professor Tim Casey from the California Western School of Law agrees, stating, “The fundamental problem is that if we think of ethics as ‘doing the right thing,’ there will always be a conflict between ethics and profit. Our systems, whether in healthcare or technology, are designed, for the most part, to increase profit, not to improve the human condition.” So how do we resolve the conflict in a way that collaboratively improves patient care without inhibiting innovation or profit? The answer as I am sure you know since you are attending today, is that the stakeholders develop and commit to an ethical framework of acceptable practices and use. Ethical frameworks that rely on patient focused security and privacy are essential to set the boundaries in which AI operates in the health sector. The framework defines the lines in the sand that we train the algorithm not to cross.

### Whose Ethics are Defining AI?

The public tends to think about artificial intelligence in a science fiction terms, with adversarial programs or robot antagonists. Our cultural perception of AI ranges from 2001 A Space Odyssey’s Hal 9000 to the Terminator. AI is not necessarily so menacing. After all, it is just algorithms and code that we develop and train to operate under conditions we specify. As trite as it sounds, artificial intelligence is imbued with the inherent, innate, and often implicit flaws, fallacies, and biases of our own intelligences. AI systems are only as good as the data we put into them and avoiding “bad” data that contains implicit racial, gender, or ideological biases is necessary to keep AI systems “fair”. Mitigating implicit and explicit racial, ideological, and other biases in AI requires transparency, collaboration, and diversity throughout the development process. Even with AI’s “human flaws” it’s potential to achieve inhuman accomplishments is not diminished. AI’s systems could hold a steadier hand at the surgical table or replicate human conversation to triage patients efficiently. It could perfectly replicate successful procedures or calculate complex risks. So how do we offset the biases embedded in AI? There is a famous adage; “think outside the box” and there is a valid argument that tools are “in the box” because they work. With AI, it isn’t an issue of thinking outside the box. Innovative strategies for AI have already been developed and are still being imagined by an engaged community. Instead, it is an issue of “how big is your box?” AI systems that operate as “black-box code” or that only draw data from a limited proprietary pool are subject to significant biases and are limited in their ability to deliver accurate conclusions. As a result, the algorithm delivers misidentifications, inaccurate conclusions, or in the case of healthcare, poor medical advice.

Instead, we need to increase the amount of available data that algorithms can access, correlate, and analyze. But we also must ensure that we are doing so in a manner that does not jeopardize the confidentiality, availability, integrity, or privacy of the data. As you can probably infer from the title of this conference, blockchain may be one of the ways that we achieve these lofty goals, but before we get there, let’s address one more question. If over the next few years, AI exponentially increased in sophistication and computational capacity, what factors would differentiate it from human providers? To put it in terms every Trekkie will recognize, what factors distinguish intelligence, logic, and judgement from compassion, empathy, and morality? The short answer, as many of you likely inferred is ethics. I am going to presume that we agree that AI should be deployed with an “ethical purpose”. What principles of ethics are necessary for a scalable healthcare framework? In my opinion, AI must be grounded in- and reflective of a distinct moral framework based on fundamental rights, societal values and the ethical principles of Beneficence (do good), Non- Maleficence (do no harm), the Autonomy of

humans, and Distributive Justice. Without ethical controls, AI could be used for profiling without consent, mass surveillance, or even the weaponization of data.

At its core, we want to use AI according to the principles of non-maleficence and respect for autonomy. But, before we even consider how AI can be used in healthcare environments, we must define the ways the data and insights should not be used. We should take a moment and recognize that the healthcare sector, more than any other critical infrastructure, is more defined by its data than its technology. Stores of PHI are the most valuable asset.

## Without Intelligent and Intentional Architecture and Design, Big Data Leads to Inequity

The public is increasingly weary of mass data collection and AI solutions. Those suspicions and apprehensions are not unfounded. Consider that between 1932 and 1972 the United States Public Health Service and the Centers for Disease Control and Prevention collected data and conducted illegal experiments on the African American population of Tuskegee Alabama. Consider how Henrietta Lacks' cells were cultivated without her knowledge or consent in 1951. In modern times, dragnet surveillance data can be aggregated with cultivated or stolen healthcare data and weaponized against a population. Consider how China leverages healthcare profiling data against their own population or how they were suspected of attempting to harvest US healthcare data at the onset of the COVID pandemic. The threat was so pronounced that Bill Evanina, Former Director of the NCSC in the ODNI, released an advisory to US hospitals, associations, and clinics warning that "Foreign powers can collect, store, and exploit biometric information from covid tests." In that last example, the firm he was responding to allegedly was offering to build "free" health centers in the US in exchange for the collection of data. This demonstrates just how valuable biometric data is compared to other digital assets. In some cases, stores of healthcare data are literally worth more than office space and infrastructure.

Even in a less malevolent use case, the public is still justified in their distrust of machine learning and big data in the healthcare space because for over a decade, stakeholders have collected data with limited notice or choice and commoditized it without concern for the security and privacy impacts. How many stories have you heard of smart device firms suffering a breach because they left failed to incorporate security controls throughout their application development lifecycle? How many stories can you think of off the top of your head where a patient's insurance premium went up or their privacy information exposed sensitive circumstances? Do you think they would have consented to the collection of their data if they had anticipated the outcomes? Do you expect they would consent to the collection and monetization of their data in the future? In order to leverage healthcare data ethically, we are going to have to change the culture that has already arisen around the use of biometric data. Patients will need to be treated as informed stakeholders capable of choice rather than as data commodities.

After all, healthcare is meant to be focused on achieving the greatest health for the most people. Artificial intelligence (AI) has the potential to revolutionize healthcare research, diagnostics, and delivery. For example, machine learning can be used to identify high-risk patients for preventive treatments, deep learning algorithms can scan radiology images to spot cancer that providers cannot see, and natural language processing is decreasing the time it takes providers to code for billing. Even non-adherence to prescriptions, a challenge that is infrequently discussed, can be addressed by AI.

Through data and devices, developers can profile patient behaviors and remind the patient to take their medication or notify their family or physician.

### Separating the Science from the Fiction

But will we see AI doctors in the near future? Probably not, but we may see AI systems that can better conduct preliminary diagnoses or route patients to the correct specialist. Essentially a more accurate and more data-driven WebMD that diagnoses the patients rather than them trying to self-diagnose. That isn't to say that we should accept all AI solutions without a healthy dose of skepticism. Healthy skepticism helps providers avoid unscalable oversight and automation bias. Learning how to identify potential flaws and errors will become essential to medical professionals as AI evolves. Broadly speaking, every AI system will need to test and set boundaries of the output. For example, with drug infusion rates, machine learning technologies continuously interpret real-time information to determine dosing requirements, but the machine does not necessarily know what an unsafe infusion rate is, and could lead to a harmful recommendation for dosing. Such an error could harm or kill a patient if not caught by the provider.

Without ethical healthcare developers, AI could fail to unscalable oversight. Unscalable oversight is the result of an AI system requiring too much time and information to effectively and efficiently accomplish its goal. The potential benefits of using AI are minimized by the amount of time and data needed to generate those results. For example, an automated insulin pump that requires a patient to input everything they ate since the last blood draw each time, they check their blood sugar levels would be exhausting to the patient and contradictive of the ease AI is supposed to have on the system.

### Equitable Healthcare AI Depends on Education as Much as Technology

AI won't replace healthcare providers, but for it to be a useful tool, it will need to be trained by medical professionals and those practitioners will need to be trained themselves in how to work with the emerging technologies. Many physicians might argue that training and using AI is not what they went to medical school to learn. Training prepared them to make diagnostic decisions to treat their patients, not understand how to develop computer algorithms or leverage derived diagnostic conclusions. However, whether they want to adapt or not, big data and AI are being increasingly integrated into clinical practices. There is rising pressure for medical professionals to be up to date with an insurmountable amount of emerging data and research. Within the decade, it will become impossible for providers to avoid understanding AI methods. We simply can't train healthcare professionals to keep up with an increasingly library of information. There is no way for medical professionals to be cognizant of and retain the plethora of data we currently expect. AI is a tool, like any other. Reading and memorizing countless journals, monitoring novel procedures and treatments being developed in hundreds of ongoing studies, and even tailoring a treatment regimen to a specific patient can all be automated by AI adoption.

By training and retraining our healthcare professionals to ethically leverage AI as a tool, we can decrease burnout, decrease workload, improve performance, and optimize patient outcomes. Medical education will need to shift from training providers to know all the data to helping them understand how to extract only the essential information from vast datasets. They will also need to be prepared for their workflow to change as AI becomes more integrated into clinical practice. To do so, future and current providers will need training on how to better understand the tools and the ethical implications associated with adopting these technologies into clinical practice. As AI becomes more integrated into clinical care, medical curricula will need to shift focus from collecting and synthesizing data to interpreting results and

emphasizing compassion. It will be critical that we define who is training and retraining healthcare professionals to be cognizant in their interactions with AI because the ethics of those instructors will transfer to their students.

### [An Multi-stakeholder Healthcare AI Ethics Framework Can Reduce Inherent Biases](#)

Consequently, a universally accepted healthcare AI ethics framework would prove instrumental in standardizing best practices and codifying expectations. AI can also ease medical education, both in preparing future physicians for a career integrating AI and in directly using AI technology in the education of medical students. Given the rise of AI, medical education may need to be reframed from a focus on knowledge recall to a focus on training students to interact with and manage AI systems. This reframing would also require diligent attention to the ethical and clinical complexities that arise among patients, caregivers, and machines.

Further without a holistic and comprehensive ethical framework and educational effort, biases in AI could compound and propagate. When providers become accustomed to accepting the guidance of an automated system without confirmatory evidence, automation bias can be introduced into practice. The provider automatically trusts the AI's output and as such does not question the accuracy of results. Such complacency is likely the strongest when the AI system either predicts that everything is normal or confirms the physician's original hypothesis. The physician is told nothing is wrong with the patient, or the physician's diagnosis was validated, so they do not question the output. Without proper training on how to understand and question AI outputs, providers can become complacent in questioning results and misdiagnose or over-diagnose a patient. Who is responsible if a misdiagnosis or AI procedure harms a patient? How will the widespread adoption of AI impact malpractice insurance rates? How will HIPAA apply to AI? We may not have the answers to these questions yet, but we need to consider that an ethical framework is necessary to standardize and codify expected behaviors. It cannot work one way at hospital A and another at hospital B. Patients need to be able to trust that the quality of care that they receive, or the security of their data will not wildly fluctuate depending upon where they have an emergency.

### [AI Must be Open and Accessible](#)

To normalize behavior and increase transparency, AI needs to be open and accessible. Providers would need to understand the methodology behind AI and its decision-making capabilities in order to know how it works, what weights it contributes to variables, how it comes to its outcome, how to interpret its findings, and be able to supervise and critically examine its results. Black box AI can limit the usability of AI technologies in clinical practice. Because the methodology behind the AI output is unclear, a provider cannot reliably assess if they want to use it in practice. The lack of transparency in the tool's methods makes it difficult for a provider to understand if the dataset used to build the tool accurately represents their patient. If the tool does not, the output of the AI system will likely be inaccurate. However, if the provider is not privy to this information, there is no way for them to decide if it is a reliable tool to use. Patients also need to be informed of what data is collected, how it is being used, and how the data is algorithmically leveraged to optimize care. In short, patients need to be informed participants who receive notice and choice. Unfortunately, the responsibility of educating and interfacing with patients may fall on healthcare professionals who themselves may not fully understand how the black box works. So how do we avoid black box systems and expand our datasets without infringing on patients' privacy or risking data exposure? Some suggest that blockchain may prove a promising solution.



## Blockchain Promises to Make Data More Coherent and Understandable

The development of AI is dependent on data, and blockchain is the technology that allows for the encrypted data to be stored in a reliable, distributed ledger. Blockchain can make data more coherent and understandable, helping trace and determine the logic behind the algorithmic decision-making process. Blockchain enhances data security, enables safe collaboration among previously non-cooperative parties (opening the “black box”) and establishes peer-to-peer networks, effectively eliminating intermediaries, cost, and time. Blockchain can provide accurate, verified data necessary to reduce bias and allows AI to become a reliable source of information and knowledge that can be used by healthcare providers, pharmaceutical companies, educational institutions, scientific researchers, non-profits, and governments.

As previously mentioned, AI is going to necessitate an increase in the amount of data collected and the mobility of that information. Healthcare data is already the most frequently targeted category of sensitive information and as AI develops, the threat landscape targeting PHI and biometric data may drastically evolve. Even when data exfiltration is not the end-goal, AI may be vulnerable to attacks that introduce biases or “poison” the algorithm to reach inaccurate or incomplete conclusions. Fortunately, just as we plan to leverage AI to improve healthcare, we may be able to use it to automate security, adapt to emerging threats, increase and enforce privacy controls, and otherwise ensure the confidentiality, availability, integrity, and privacy of biometric data.

Tuning the access controls of machine learning helps train the AI to discern patterns from the information ingested. However it requires large amounts of data to learn accurately and effectively and as a result, necessitates the collection and storage of large data pools that are at risk of theft and exploitation. This risk makes access controls a particular area of concern. Consider:

- Who can see that data?
- Who has permission to manage the data?
- Who has permission to make changes to the rules, algorithms, or models the machine is using to learn?
- What other applications, systems, or enterprises will access your information?
- Do you understand all the people and entities with access, and are you ensuring the security and privacy controls implemented are appropriate for the level of access necessary to each?

Now, consider the layers of risk associated with the developer’s processes, practices, and policies?

- Do you know who built the algorithm or model you’re using?
- How can you trust them?
- Do you trust their supply chain?
- What procedures can you put in place to make sure the people giving you this information are doing so securely and with the best intentions?
- How can you combat the biases that may have been incorporated into the algorithm without your knowledge?
- How vulnerable is the AI to misinformation or exploitation?
- Was security incorporated throughout the development lifecycle?
- Was application development subcontracted to any other firms?
- How long is data retained?
- How is it disposed of?

What controls are ensuring the integrity of the information fed into your algorithm? AI depends on the depth of your data set. If your database only includes information from a cohort group of one million men, then your clinical decision support for women and children may be weak. It's important to consider these implicit biases and plan methodologies to mitigate their impacts. Moreover, the algorithm itself must be analyzed to ensure that nothing about the way it's coded produces bias.

## Communication is Key to Understanding Limits and Goals

And finally, how do security professionals and developers communicate concerns to corporate boards and executive leadership? Not only can they use their knowledge to discuss the benefits of AI with the board, but they can also highlight ways to better protect the privacy and security of patient data. All purchases should go through the regular IT requisition process regardless of who's championing the technology. This helps ensure all relevant parties understand the risks involved, establish plans to mitigate them, and ensure that key decision makers understand the societal, legal, moral, and technological limits of the solution. AI and machine learning are not panaceas. Not all technology is suitable for all uses and more importantly, not all data is appropriate for all business purposes. Ethics relies on boundaries that cannot be crossed no matter the potential market gains. The data and tools designed for clinical decision support may only be designated for research or for a limited purpose.

## Stakeholders Each Have a Role and Responsibilities in the Ethical Development of AI

An actionable framework needs "teeth." After all, developing an ethical framework that is entirely voluntary or that has no traction may be an exercise in futility. Patients expect a certain measure of standardized care; therefore, the ethical framework will need a mechanism to incentivize near-unanimous adoption. Regulators and legislators could adopt the framework and require compliance similar to HIPAA; but if that were to happen, we must remain vigilant that the tenets of the framework were not reduced to an ineffective minimalism because an ethical framework should not rely on the lowest possible expectations. It should instead prioritize the security and privacy of patient data and the accountability of stakeholders. Lastly, when collaborating with technology partners, providers must ensure that those developers also adhere to the ethical framework; especially if the technology firm would act as third-party in the environments. Otherwise, the entire ethical framework could be bypassed by non-participant organizations that unethically collect, leverage, or commoditize data in ways that patients did not knowingly consent.

## Conclusion - AI Promises Progress, But It Is Not a Panacea

Artificial Intelligence is not a panacea and its impact on healthcare could prove positive or negative depending on whether ethics are standardized, how they are selected, if they are enforced, and how they are applied. AI is a tool that like any software must be fostered and developed with great care and responsibility. Without standardization in the development, adoption, application, and enforcement of AI ethics in healthcare, the risk for asymmetric outcomes, disadvantaging disparaged communities may be high. Fortunately, developers, healthcare professionals, agency regulators, and legislators already have the tools necessary to craft, implement, and enforce AI ethics provided they communicate, collaborate, and act with foresight.

## Resources

- [1]"Program | IEEE Healthcare: Blockchain & AI", *Attend.ieee.org*, 2022. [Online]. Available: <https://attend.ieee.org/healthcare-blockchain-ai/program/>. [Accessed: 01- Jun- 2022].
- [2]A. Cahana, "To Keep AI Ethical We Need To Use Blockchain", *Medium*, 2019. [Online]. Available: <https://medium.com/crypto-oracle/to-keep-ai-ethical-we-need-to-use-blockchain-aaf2733626cd>. [Accessed: 01- Jun- 2022].
- [3]M. Robert Pearl, "How AI Can Live Up To Its Hype In The Healthcare Industry", *Forbes*, 2020. [Online]. Available: <https://www.forbes.com/sites/robertpearl/2020/02/24/ai-hype/?sh=13f74383458e>. [Accessed: 01- Jun- 2022].
- [4]"What if blockchain could guarantee ethical AI?", *Europarl.europa.eu*, 2020. [Online]. Available: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/656334/EPRS\\_ATA\(2020\)656334\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/656334/EPRS_ATA(2020)656334_EN.pdf). [Accessed: 01- Jun- 2022].
- [5]E. Garvin, "Ethical Concerns of AI in Healthcare: Can AI Do More Harm Than Good?", *Hitconsultant.net*, 2019. [Online]. Available: <https://hitconsultant.net/2019/08/06/ethical-concerns-of-ai-in-healthcare-can-ai-do-more-harm-than-good/>. [Accessed: 01- Jun- 2022].
- [6]"Consent-as-a-Service", *Live With AI*, 2022. [Online]. Available: <https://livewithai.org/consent-as-a-service/>. [Accessed: 01- Jun- 2022].
- [7]"Leveraging AI and Blockchain to Transform Healthcare | Innoplexus", *Innoplexus*, 2022. [Online]. Available: <https://www.innoplexus.com/news/leveraging-ai-and-blockchain-to-transform-healthcare/>. [Accessed: 01- Jun- 2022].
- [8]"Revolutionizing Healthcare with Blockchain and Artificial Intelligence", *Cbcamerica.org*, 2020. [Online]. Available: <https://www.cbcamerica.org/blockchain-insights/revolutionizing-healthcare-with-blockchain-and-artificial-intelligence>. [Accessed: 01- Jun- 2022].

- [9]"AI, machine learning, and blockchain are key for healthcare innovation", *Health Europa*, 2020. [Online]. Available: <https://www.healtheuropa.eu/ai-machine-learning-and-blockchain-are-key-for-healthcare-innovation/99990/>. [Accessed: 01- Jun- 2022].
- [10]M. Smolaks, "How AI and blockchain combine to improve healthcare", *AI Business*, 2019. [Online]. Available: [https://aibusiness.com/document.asp?doc\\_id=761099](https://aibusiness.com/document.asp?doc_id=761099). [Accessed: 01- Jun- 2022].
- [11]M. Goirand, E. Austin and R. Clay-Williams, "Implementing Ethics in Healthcare AI-Based Applications: A Scoping Review", *Science and Engineering Ethics*, vol. 27, no. 5, 2021. Available: 10.1007/s11948-021-00336-3.
- [12]D. Char, "Challenges of Local Ethics Review in a Global Healthcare AI Market", *The American Journal of Bioethics*, vol. 22, no. 5, pp. 39-41, 2022. Available: 10.1080/15265161.2022.2055214.
- [13]J. Morley et al., "The Ethics of AI in Health Care: A Mapping Review", *SSRN Electronic Journal*, 2020. Available: 10.2139/ssrn.3830408.
- [14]T. Saheb, T. Saheb and D. Carpenter, "Mapping research strands of ethics of artificial intelligence in healthcare: A bibliometric and content analysis", *Computers in Biology and Medicine*, vol. 135, p. 104660, 2021. Available: 10.1016/j.combiomed.2021.104660.
- [15]A. Fiske, D. Tigard, R. Müller, S. Haddadin, A. Buyx and S. McLennan, "Embedded Ethics Could Help Implement the Pipeline Model Framework for Machine Learning Healthcare Applications", *The American Journal of Bioethics*, vol. 20, no. 11, pp. 32-35, 2020. Available: 10.1080/15265161.2020.1820101.
- [16]C. Ho and R. Malpani, "Scaling up the Research Ethics Framework for Healthcare Machine Learning as Global Health Ethics and Governance", *The American Journal of Bioethics*, vol. 22, no. 5, pp. 36-38, 2022. Available: 10.1080/15265161.2022.2055209.
- [17]A. Panesar, *Machine learning and AI for healthcare*. [Place of publication not identified]: Apress, 2021, pp. 207-247.

- [18]B. Giovanola and S. Tiribelli, "Beyond bias and discrimination: redefining the AI ethics principle of fairness in healthcare machine-learning algorithms", *AI & SOCIETY*, 2022. Available: 10.1007/s00146-022-01455-6.
- [19]H. Siala and Y. Wang, "SHIFTing artificial intelligence to be responsible in healthcare: A systematic review", *Social Science & Medicine*, vol. 296, p. 114782, 2022. Available: 10.1016/j.socscimed.2022.114782.
- [20]W. Rogers, H. Draper and S. Carter, "Evaluation of artificial intelligence clinical applications: Detailed case analyses show value of healthcare ethics approach in identifying patient care issues", *Bioethics*, vol. 35, no. 7, pp. 623-633, 2021. Available: 10.1111/bioe.12885.
- [21]B. Shneiderman, "Bridging the Gap Between Ethics and Practice", *ACM Transactions on Interactive Intelligent Systems*, vol. 10, no. 4, pp. 1-31, 2020. Available: 10.1145/3419764.
- [22]M. Schildt, "Ethics of Using AI in Healthcare Diagnostics - a scoping review", Master of Business Administration, Metropolia University of Applied Sciences, 2022.
- [23]J. Amann, A. Blasimme, E. Vayena, D. Frey and V. Madai, "Explainability for artificial intelligence in healthcare: a multidisciplinary perspective", *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, 2020. Available: 10.1186/s12911-020-01332-6.
- [24]C. Oxholm, A. Christensen and A. Nielsen, "The Ethics of Algorithms in Healthcare", *Cambridge Quarterly of Healthcare Ethics*, vol. 31, no. 1, pp. 119-130, 2022. Available: 10.1017/s0963180121000864.
- [25]J. Wadden, "Defining the undefinable: the black box problem in healthcare artificial intelligence", *Journal of Medical Ethics*, pp. medethics-2021-107529, 2021. Available: 10.1136/medethics-2021-107529.
- [26]J. Guan, "Artificial Intelligence in Healthcare and Medicine: Promises, Ethical Challenges, and Governance", *Chinese Medical Sciences Journal*, vol. 34, no. 2, pp. 76-83, 2019. Available: 10.24920/003611.



[27]K. Siau and W. Wang, "Artificial Intelligence (AI) Ethics", *Journal of Database Management*, vol. 31, no. 2, pp. 74-87, 2020. Available: 10.4018/jdm.2020040105.

[28]J. Morley and L. Floridi, "NHS AI Lab: Why We Need to Be Ethically Mindful About AI for Healthcare", *SSRN Electronic Journal*, 2019. Available: 10.2139/ssrn.3445421.

[29]A. Jobin, M. Ienca and E. Vayena, "The global landscape of AI ethics guidelines", *Nature Machine Intelligence*, vol. 1, no. 9, pp. 389-399, 2019. Available: 10.1038/s42256-019-0088-2.

[30]S. Reddy, S. Allan, S. Coghlan and P. Cooper, "A governance model for the application of AI in health care", *Journal of the American Medical Informatics Association*, vol. 27, no. 3, pp. 491-497, 2019. Available: 10.1093/jamia/ocz192.

[31]M. Smallman, "Multi Scale Ethics – Why we need a sociological approach to the ethics of AI in healthcare at different scales.", *SocArXiv*, 2022. Available: 10.31235/osf.io/uj6my [Accessed 1 June 2022].

[32]E. Frost, R. Bosward, Y. Saint James Aquino, A. Braunack-Mayer and S. Carter, "Page 1/11 Is Healthcare AI Research Engaging Publics In Conversations About Ethics? Protocol For A Scoping Review", University of Wollongong, 2021.

[33]M. Ryan, "In AI We Trust: Ethics, Artificial Intelligence, and Reliability", *Science and Engineering Ethics*, vol. 26, no. 5, pp. 2749-2767, 2020. Available: 10.1007/s11948-020-00228-y.

[34]S. Duke, "Deny, dismiss and downplay: developers' attitudes towards risk and their role in risk creation in the field of healthcare-AI", *Ethics and Information Technology*, vol. 24, no. 1, 2022. Available: 10.1007/s10676-022-09627-0.

[35]G. Karimian, E. Petelos and S. Evers, "The ethical issues of the application of artificial intelligence in healthcare: a systematic scoping review", *AI and Ethics*, 2022. Available: 10.1007/s43681-021-00131-7.

[36]N. Terry, "Of Regulating Healthcare AI and Robots", *SSRN Electronic Journal*, 2019. Available: 10.2139/ssrn.3321379.

- [37]E. LaRosa and D. Danks, "Impacts on Trust of Healthcare AI", in *AIES '18: Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, 2018, pp. 210-215.
- [38]T. Lysaght, H. Lim, V. Xafis and K. Ngiam, "AI-Assisted Decision-making in Healthcare", *Asian Bioethics Review*, vol. 11, no. 3, pp. 299-314, 2019. Available: 10.1007/s41649-019-00096-0.
- [39]F. Gille, A. Jobin and M. Ienca, "What we talk about when we talk about trust: Theory of trust for AI in healthcare", *Intelligence-Based Medicine*, vol. 1-2, p. 100001, 2020. Available: 10.1016/j.ibmed.2020.100001.
- [40]V. Sounderajah et al., "Ethics methods are required as part of reporting guidelines for artificial intelligence in healthcare", *Nature Machine Intelligence*, vol. 4, no. 4, pp. 316-317, 2022. Available: 10.1038/s42256-022-00479-3.
- [41]Bartoletti, I. (2019). AI in Healthcare: Ethical and Privacy Challenges. In: Riaño, D., Wilk, S., ten Teije, A. (eds) Artificial Intelligence in Medicine. AIME 2019. Lecture Notes in Computer Science(), vol 11526. Springer, Cham. [https://doi.org/10.1007/978-3-030-21642-9\\_2](https://doi.org/10.1007/978-3-030-21642-9_2)
- [42]Leslie, David, Understanding Artificial Intelligence Ethics and Safety: A Guide for the Responsible Design and Implementation of AI Systems in the Public Sector (June 10, 2019). Available at SSRN: <https://ssrn.com/abstract=3403301> or <http://dx.doi.org/10.2139/ssrn.3403301>
- [43]Lehmann L.S. (2022) Ethical Challenges of Integrating AI into Healthcare. In: Lidströmer N., Ashrafian H. (eds) Artificial Intelligence in Medicine. Springer, Cham. [https://doi.org/10.1007/978-3-030-58080-3\\_337-2](https://doi.org/10.1007/978-3-030-58080-3_337-2)
- [44]A. C. Chase, "Ethics of AI: Perpetuating Racial Inequalities in Healthcare Delivery and Patient Outcomes", *VIB*, vol. 6, Apr. 2020.
- [45]Fukuzumi, S., Jinno, M., Inagaki, K., Maeda, H., Mizukami, T., Sakura, O. (2019). Extraction of New Guideline Items from the View Point of ELSI (Ethics, Legal, Social Issues) for Service Utilized AI—Focus on Healthcare Area. In: Yamamoto, S., Mori, H. (eds) Human Interface and the Management of Information.

Information in Intelligent Systems. HCII 2019. Lecture Notes in Computer Science(), vol 11570. Springer, Cham. [https://doi.org/10.1007/978-3-030-22649-7\\_38](https://doi.org/10.1007/978-3-030-22649-7_38)

[46]Rana, A., Goedmakers, C.M.W., Smith, T.R. (2021). Artificial Intelligence and Healthcare Ethics. In: Honeybul, S., Kolas, A.G. (eds) Traumatic Brain Injury. Springer, Cham. [https://doi.org/10.1007/978-3-030-78075-3\\_31](https://doi.org/10.1007/978-3-030-78075-3_31)