Navigating the Challenges of AI in Medical Devices: A Comprehensive Study

Yiwen Li[1], Luya Wang[2]

Department of Statistical Sciences, University of Toronto, Toronto, ON, Canada
Department of Computer Sciences, University of Toronto, Toronto, ON, Canada

ABSTRACT

The integration of Artificial Intelligence into medical devices adds unmeasurable potential to healthcare systems through different aspects, including data-driven diagnostics, treatment, and monitoring. Nevertheless, introducing AI in delicate medical contexts also raises unavoidable challenges in ethics, policies, and technology that require mindful regulation. This report provides an overview of key issues involved in AI-enabled medical device development based on a literature review. According to the literature review, it's clear that there are gaps in current regulatory frameworks in the United States and Canada in providing effective oversight and guidance for fast-evolving AI systems. System opacity and the lack of interpretability in complex algorithms limit trust and accountability. Besides, biases in both algorithms and datasets, along with privacy risks, can impact performance and safety. Additional concerns, including cybersecurity vulnerabilities, unclear legal liability, and influences on trust relationships, will also be discussed in this report. Coordinated efforts are needed across policy, technical, and social domains to ensure the responsible development of AI healthcare technologies.

1 INTRODUCTION

As technology evolves rapidly in recent times, medical devices are now playing a crucial role in diagnosing, treating, and monitoring medical conditions. From simple tools like blood pressure monitors to recent innovations like robotic surgeries, medical devices impact nearly every facet of patient care, significantly advancing therapeutic capabilities and improving the overall quality of life for individuals. With the rapid emergence of artificial intelligence technologies, the integration of AI has transformed the scope and utility of medical devices. AI technologies offer the capability to process vast volumes of data, identify complex patterns, and generate valuable insights with remarkable accuracy, augmenting medical devices to unprecedented levels.

Companies and healthcare institutions are increasingly adopting AI-based medical devices to harness data-driven insights and provide more accurate and timely medical interventions. However, the adoption of AI into medical devices also introduces critical considerations and challenges around existing regulatory frameworks, data-related concerns, bias issues, algorithmic transparency, system security, clinical trust, and ethical development practices. Without diligent focus on these impacts, AI systems risk exacerbating disparities and inequities. Active commitment to ethical, trustworthy AI that centers patient interests is imperative. In this case, finding a balance between innovation and patient safety is paramount in this journey toward AI-enabled medical devices.

In light of these potential challenges, this report provides a high-level overview of the key challenges faced by AI-enabled medical devices in healthcare, based on literature reviews on this topic. The focus is on summarizing the core issues and concerns that span technological, ethical, regulatory, and social domains, highlighting the need to establish a more sophisticated regulation framework.

2 RESEARCH QUESTIONS AND METHOD

We will explore the following two key research questions surrounding the key issues involved in the AI-based medical devices development process:

- What/Who are the stakeholders involved in during this development lifecycle?
- What are the challenges of implementing AI-based medical devices?

During the software development life cycle, there will be different stakeholders with different responsibilities involved in the process. Thus, the first research question

sought to identify the key stakeholders involved to explore what are the different challenges faced by different stakeholders. The second research question focused on summarizing the main challenges around the responsible implementation of AI in healthcare contexts.

To investigate these research questions, this literature review was performed by searching through platforms, including Google Scholar, ACM Digital Library, and IEEE Xplore, collating a collection of highly relevant papers. Initial keyword searches included terms like 'artificial intelligence,' 'machine learning,' 'medical devices,' 'regulation,' and 'challenges'. As the search process went on, more terms like 'MIMIC,' and 'bias' were added. The final 34 papers were selected and evaluated based on relevance to the research questions.

The collected literature encompassed research studies, review papers, case studies, and analyses focused on AI in healthcare. Common themes around stakeholder roles and challenges were identified across the papers, which could provide a comprehensive overview of the current state of knowledge based on empirical evidence and expert analysis from the field.

By answering these questions, we hope to provide insights for companies, regulators, and researchers to establish more sophisticated regulatory frameworks.

3 Discussion

RQ1: What/Who are the stakeholders involved during this development life-cycle?

Although there is no paper discussing the roles involved in the development lifecycle systematically, by identifying the common theme across papers, a complex landscape of stakeholders that play crucial roles has been revealed. Key stakeholders span multiple sectors, including device manufacturers and developers responsible for developing the technologies, healthcare institutions and staff who utilize them for patient treatment, regulators and policymakers who oversee the safety, patients whose data and health are impacted, and researchers who study these systems. Meaningful participation by providers and patient groups is necessary to address needs and build trust. Regulators must maintain flexible governance as technologies rapidly evolve. Continual efforts are needed for manufacturers to ensure safety and efficacy. The analysis highlighted the need for active collaboration between these diverse stakeholders throughout the design, deployment, and oversight of AI-based medical devices to optimize the outcomes while minimizing harm. Future research could focus on optimizing relationships between stakeholders and communication strategies to support responsible AI integration.

RQ2: What are the challenges of implementing AI-based medical devices?

Upon reviewing these 34 papers, some common themes for challenges involved in safely and effectively integrating AI in healthcare contexts can be identified. There are discussions going on with the gaps existing in the current regulation frameworks in both the United States and Canada, especially regarding the ambiguity of regulation terms, the pre-market approval process, and post-market surveillance. One major cluster of challenges stems from data considerations, including privacy risks with sensitive patient information and unreliable data that impairs algorithm performance. Apart from data bias, algorithmic bias is another type of bias that could be easily ignored but has huge potential impacts on model performance as well. The literature also emphasized a lack of transparency and explainability in AI systems, which can undermine clinician and patient trust. Additional challenges span the difficulty of ensuring robust cybersecurity, unclear legal liability when adverse events occur, and the impacts on trust relationships when utilizing AI outputs.

The analysis revealed the need for a multifaceted approach to responsible AI governance and deployment that bridges technical and social considerations. While AI enables significant healthcare advances, actively addressing the challenges identified is crucial for developing ethical, safe, and effective AI-based medical software that improves access and outcomes across populations. Future research can focus on building strategies that include updated regulatory frameworks focused on AI system lifecycles rather than just pre-market approval, stronger data governance policies, investments in explainable and transparent AI design, extensive testing on diverse populations, and community participation to build trust.

I. Current Regulation Framework

Ambiguity in Regulations

While innovation in AI-enabled healthcare technologies is rapidly accelerating, regulatory frameworks are lagging behind in providing effective oversight and guidance. In the United States, the Food and Drug Administration (FDA) is the regulatory body that is responsible for the oversight of medical devices and software but has been criticized for lacking clarity in AI regulations. Ambiguous language used in writing the regulations leads to multiple interpretations, causing confusion for companies seeking to meet regulatory requirements properly. One study discussed that manufacturers struggle to identify and understand relevant regulatory requirements during the development lifecycle, as legal texts contain inherent ambiguities when drafted by legislative bodies and sometimes could be interpreted differently by people from different backgrounds [18]. Setting up clear regulation rules is fundamental, as a proper understanding of the rules is the cornerstone of regulatory compliance. And making timely modifications in response to scientific and technological advancements is also essential. However, regulators and policymakers still face challenges in adequately defining and scoping key concepts like whether AI software integrated into a medical context could be considered a medical device [10]. When attempting to regulate any new or emerging fields, the definition, including proper scope and boundaries, is definitely one of the essential aspects that need to be considered [10]. To get a better understanding of the dilemma faced in defining a new and emerging matter, Internet of Things devices could be a good example. As one of the emerging technologies, Internet of Things devices have been utilized in various domains, even in the healthcare domain. With embedded AI features, the Internet of Health becomes more powerful, which would also need to be regulated. In this case, the first thing to be considered is whether the Internet of Health Things still falls into the definition of 'medical devices' [21]. There are other issues that need to be addressed, like overlaps across the FDA and other agencies' policies which cause inconsistencies in how IoHT and AI software are regulated [21]. These gaps in current frameworks regarding both ambiguity and the convergence of emerging new technologies hamper regulators' capacity to provide effective, timely oversight as innovation rapidly outpaces policy. Without updated regulations designed intentionally for AI systems, safety risks and barriers to beneficial adoption may result from a lack of clear guidance for manufacturers and healthcare providers.

Risk Assessment and post-market surveillance

Before any AI-based medical devices can be released onto the market, they need to be evaluated for safety by regulatory bodies. The evaluation steps can be roughly categorized into two main phases: pre-market approval process and post-market surveillance. The pre-market approval process has limitations in evaluating evolving medical devices, especially in risk assessment. Risk assessment is one of the most fundamental components in the pre-market approval process. In both the United States and Canada, the risk profile was initially selected by the company [17][13], which would pose the risk that companies may select low or medium-risk profiles initially to avoid providing explicit evidence of product safety and efficacy. There is no public documentation on how and to what extent Health Canada will review the selection process [17]. As mentioned in the research paper, there are a considerable number of AI devices that get cleared through the 501(k) 'equivalence' review pathway [14]. With the 501(k) pathway, companies are allowed to submit clinical evaluation documentation indicating the equivalence or similarity to an approved device to get approval. This pathway seems to help companies select their risk profiles, but there are still issues that need to be carefully regulated. On one hand, one study shows that there are devices reviewed through the 510(k) process that got approved without being tested in clinical trials, which means the devices were tested with nonclinical testing for proof of equivalence to the marketed devices [23]. This could be potentially harmful to patients' safety and lead to serious problems as it's extremely risky to release any medical devices to the market without clinical trials. On the other hand, as Vokinger proposed, with special characteristics of the 510(k) pathway, there could be chains of medical devices that got approved by declaring substantial equivalence, but eventually, diverge substantially from the original device over years or decades [14]. Worsely, most of the device documentation does not even declare the usage of any AI components [14]. The gaps in the pre-market approval process give the manufacturers chances to release AI-based medical devices without explicitly declaring any AI components [14][22]. Overall, because of the complexity and the black-box nature of AI algorithms, it is challenging for the FDA to finish the approval process in a timely manner **[10].** Post-market surveillance has been another challenge for both companies and regulators. As AI algorithms become much more complicated and less transparent, it's challenging to detect or report abnormal behavior or defects. And the fact that AI applications evolve over time with more data feeding and knowledge makes

post-market surveillance even harder. The lack of regulatory guidance on post-market monitoring, testing, and reporting has become a serious challenge for regulators, manufacturers, and healthcare professionals.

II. Data-related issues

Privacy

Privacy has always been a central concern with healthcare data used for AI as patient records contain highly sensitive personal information. Despite patient consent being required for data collection and access most of the time, some patients still worry about downstream usage risks like denial of insurance or effects on potential employment [17]. However, not all sensitive data is being shared with patient consent or knowledge. One study found that patients often have no idea of whether their data will be shared with other healthcare-related parties and even have little control over whether the sensitive data will be shared [6]. The study further noted that there are patients' data regularly shared without patients' knowledge between companies and healthcare systems like Ascension Health shared the EHR data with Google, highlighting gaps in data usage transparency [6]. While de-identification through anonymization provides some privacy protection, it's not always possible to do so and there is no 100% guarantee by any existing methods for data protection [17][9]. One study mentioned that a number of studies have discussed the capability of advanced computational strategies and machine learning algorithms to re-identify "anonymous" individuals with high accuracy, providing a successful example of re-identifying anonymous health data [5]. This enables involuntary data exploitation, as consent is not legally required for de-identified datasets [17]. There are also other concerns of privacy invasion, such as potential data breaches with big data analytics, the change of purpose in using sensitive data over time, and accidental data leaks because of third-party/business transfer [12][5][4]. It's worth noting that as IoHT devices have come into people's lives and turned users' bodies into a data platform, there should be clear legal clarification on what kind of personal health data can be collected from their daily life habits [21]. Though emerging technical safeguards like encryption and blockchain offer promise, optimizing both privacy and utility remains an open challenge. More control over data-sharing decisions from patients is required to align with personal privacy preferences. However, it is clear that current regulatory frameworks provide insufficient oversight, and failing to address privacy concerns with AI integration risks public trust and healthcare equity.

Reliability of data

Obtaining high-quality, unbiased, and representative datasets is extremely important to train robust AI systems with high performance. However, it is usually a challenge in the healthcare domain. For any complex AI algorithm, having enough data is essential. For many medical conditions, especially rare diseases or medical conditions, there is simply not enough real-world data available to model and test AI algorithms accurately. In this case, accessing data across platforms is necessary. However, accessing large amounts of data across platforms might be difficult due to different policies or regulations from different institutions. Due to limited data access, AI developers may use datasets from unknown or poorly documented sources or even potentially collect unethical or illegal data [10]. For instance, as the regulation rules for accessing data might be different across institutions and provinces, it's hard to access data across Canada, which may force AI developers to utilize foreign datasets to get sufficient data for AI development [17]. But even with sufficient datasets, quality issues persist. Medical data frequently suffers from problems like incompleteness, inconsistencies, errors, and lack of context. Missing fields or variability in formats for things like test orders, prescriptions, and doctor's notes can negatively impact model performance. Furthermore, Datasets also frequently fail to represent diverse demographics, leading to algorithms that work for majority groups but underserve marginalized communities, which negatively impacts model performance and generalizability and could be potentially harmful to underrepresented groups. It is clear that guidelines on data quality are missing and need to be regulated in the future [1]. Proactive efforts to curate high-quality, unbiased, and representative training data are essential but face substantial challenges in healthcare contexts. Failing to address these data issues risks patient harm and may magnify existing disparities.

Bias

While dataset bias has been a major concern, other sources of bias also pervade healthcare AI systems that are sometimes being ignored or overlooked. As we discussed in the previous section, medical datasets frequently

underrepresent minority groups. A case study was performed on a benchmark model, finding that the model had significantly lower prediction performance on black people in all assessment stages, which seems to be caused by the underrepresentation of Black patients in datasets [8]. And even if this underrepresentation issue can be mitigated by training with a larger amount of datasets, sometimes bias still exists in the data itself. For example, one study shows that there are gender and ethnicity biases during communication between physicians and patients [7]. In this case, if these communication prescriptions are used for AI models, these underlying biases could affect the performance of the model and will be hard to identify. On the other hand, developing AI models involves many subjective decisions that can incorporate existing social biases around race, gender, age, etc., whether consciously or not [16]. Bias also creeps in through assumptions in model architecture choices and proxy variables. For instance, a study shows that in a widely used commercial algorithm, bias was detected in classifying Black patients' illness conditions at a given risk score, which was caused by the selection of proxies with healthcare costs [24]. Such algorithmic biases are challenging to recognize or test for during the development phases. And there are no clear regulations or policies on algorithm bias [17]. Once deployed, biased AI risks perpetuating injustice through feedback loops as model predictions influence real-world data distribution. Though some governments have enacted anti-discrimination regulations, few mechanisms exist to proactively prevent algorithmic bias in healthcare. Understanding how human subjectivity infects the entire pipeline is key to developing fair, ethical AI systems that do not cause disproportionate harm. More rigorous requirements are needed surrounding audits for prejudice, testing on diverse populations, and community participation.

Transparency

The inherent complexity of many modern AI systems leads to challenges in interpretability and transparency on multiple levels. Techniques like deep neural networks function as inscrutable "black boxes", making it difficult to fully trace how AI algorithms process the data and even harder to be explained to others like regulatory bodies or healthcare providers. And identifying or tracing the source of incorrectness in a meaningful way is also challenging for complex models [2]. On the other hand, this system's opacity and the lack of explainability also pose significant challenges to healthcare providers, where clinicians and physicians sometimes might not know the rationale behind AI decisions, treatments, or recommendations to establish trust and accountability [11][20]. Without providing a logical explanation of how particular decisions or recommendations are derived by the AI algorithms, medical malpractice and product liability legal issues might arise [15]. Transparency to patients is also necessary. When making decisions using any AI algorithm, patient information needs to be input into the software or devices. It should be transparent to the patient that their information will be used in the AI algorithms and the decisions or recommendations they get might be interfered with from AI computation results. Although manufacturers still struggle with making AI algorithms more transparent while maintaining high performance, there are no explicit rules or frameworks for measuring and regulating transparency and explainability.

III. Cyber Security

The increasing integration of AI, medical devices, IoT sensors, and other connected technologies exponentially expands the attack surface and cyber risks for healthcare systems. Although cybersecurity is now becoming an important factor to be considered these days, many existing clinical systems and medical devices were developed without cybersecurity consideration as one of the implementation priorities, leading to vulnerabilities. As these legacy systems interact with AI-based medical devices and get network connectivity for health data sharing, more threats emerge [1]. Connected devices provide new vectors for cybercriminals to infiltrate systems and access sensitive patient records, and could be potentially life-threatening if compromised, manipulated, or fooled by adversarial inputs. With the rapid emergence of cloud computing, centralizing sensitive health data for AI training and inference also creates attractive targets for hackers to steal records. Robust cybersecurity protocols and resilience testing are critical across the entire product lifecycle of AI-enabled medical devices. However, security protocols and capacity might be inconsistent among different institutions. As mentioned in the paper, since healthcare systems in Canada are operated by various entities, the security capacity is varied, leading to potential vulnerabilities [17]. Security must be treated as a core functional requirement, as any attacks could lead directly to patient harm.

IV. Liability

There have been liability concerns arising with the emergence of AI technology. With the growing integration in different domains, AI models should be built and utilized in a morally accountable manner to meet social standards and values [19]. Apart from moral accountability, legal accountability has become another issue that needs to be addressed timely. The autonomous and adaptive nature of AI systems poses significant legal challenges in assigning responsibility when harm occurs. When an AI diagnosis or treatment recommendation results in patient injury or death, it becomes very difficult to conclusively determine liability under current medical malpractice frameworks [3]. Furthermore, the complex supply chain of stakeholders, including developers, device manufacturers, healthcare systems, and clinicians, makes accountability even more obscured [1]. Legislative reforms are needed to apportion liability fairly based on the unique risks of these technologies.

V. Trust

Building appropriate trust between clinicians and AI systems is crucial for effective adoption and impact. Both overtrusting AI, allowing errors of omission through over-reliance, and underthrusting it, rejecting potentially valuable insights, are risks to be mitigated through training and experience. There are different factors that affect trust in AI, which vary from human characteristics to the characteristics of AI systems [19]. Without enough transparency on the AI model, like the explanation of how the model works generally and real-world performance bounds, clinicians struggle to establish proper trust in model outputs. Clear communication about AI limitations and intended usages is essential to avoid unrealistic expectations that undermine provider confidence. There have been concerns that with the rapid evolution of AI technology, precision, and efficiency will eventually become more valued than empathy and professional judgment, substituting physicians' judgment [3]. What should be clear is that AI should be operated in an assisting role, not replacing human expertise and ethical reasoning. In this case, designing AI systems focused on human-in-the-loop enhancement rather than automation may enable higher levels of clinician acceptance and adoption. With human judgment guiding AI use for selected supportive tasks, tangible benefits become apparent without threatening professional integrity or independence.

4 LIMITATIONS & FUTURE WORK

While this report aims to provide a comprehensive overview of key challenges faced by AI-based medical devices, there are some limitations to note. The literature review, while broad, may have missed issues not widely studied yet. The analysis relied on published research, so recent developments and ongoing projects may be missed. Highly dynamic topics like cybersecurity vulnerabilities and algorithmic biases require constant investigation as new threats and forms of unfairness rapidly emerge. Furthermore, this paper focused more on theoretical discussion compared to qualitative data, such as surveys of patient attitudes and clinician experiences with real-world AI systems, because of the limitation of the selected paper. Follow-up work could include interviews with stakeholders like manufacturers and regulators for deeper insights. Future studies should continue investigating open problems like accountability, participation of minority groups, and establishing adaptive regulation rules or frameworks for building responsible AI systems in the healthcare context. Responsible AI-enabled healthcare requires sustained, coordinated efforts between researchers, providers, policymakers, and communities.

5 CONCLUSIONS

Realizing the potential of AI in healthcare comes with significant technological and ethical challenges requiring diligent focus from all stakeholders to overcome. Establishing sophisticated and adoptive regulation frameworks without ambiguities is the foundation of responsible AI development. Ensuring access to comprehensive, high-quality, and unbiased datasets is essential for developing robust models capable of generalizing safely across diverse populations. Even with strong datasets, enhancing explainability and transparency in complex AI models remains difficult but necessary for clinical acceptance and regulatory oversight. As AI integration expands, cybersecurity protections and resilience against attacks must be prioritized to avoid potential life-threatening breaches. Cultivating appropriate trust through training, communication, and purposeful human-AI collaboration helps enhance care quality without undermining professional judgment and independence. Overcoming these challenges will allow society to deploy AI capabilities in medicine ethically and equitably while remaining vigilant against risks on the path forward.

REFERENCES

[1] Andrew Mkwashi and Irina Brass. 2022. The Future of Medical Device Regulation and standards: Dealing with critical challenges for connected, Intelligent Medical Devices. *SSRN Electronic Journal* (2022). DOI:http://dx.doi.org/10.2139/ssrn.4226057

[2] Anon. Ai in medical devices: Key challenges and global responses. Retrieved September 2, 2023 from https://www.mhc.ie/latest/insights/ai-in-medical-devices-key-challenges-and-global-responses

[3] Anto Čartolovni, Ana Tomičić, and Elvira Lazić Mosler. 2022. Ethical, legal, and social considerations of AI-based medical decision-support tools: A scoping review. *International Journal of Medical Informatics* 161 (2022), 104738. DOI:http://dx.doi.org/10.1016/j.ijmedinf.2022.104738

[4] Blake Murdoch, Allison Jandura, and Timothy Caulfield. 2022. Privacy considerations in the Canadian regulation of commercially-operated Healthcare Artificial Intelligence. *Canadian Journal of Bioethics* 5, 4 (2022), 44. DOI:http://dx.doi.org/10.7202/1094696ar

[5] Blake Murdoch. 2021. Privacy and artificial intelligence: Challenges for protecting health information in a new era. *BMC Medical Ethics* 22, 1 (2021). DOI:http://dx.doi.org/10.1186/s12910-021-00687-3

[6] Brad Morse et al. 2023. Patient and researcher stakeholder preferences for use of electronic health record data: A qualitative study to guide the design and development of a platform to honor patient preferences. *Journal of the American Medical Informatics Association* 30, 6 (2023), 1137–1149. DOI:http://dx.doi.org/10.1093/jamia/ocad058

[7] David M. Markowitz. 2022. Gender and ethnicity bias in medicine: A text analysis of 1.8 million Critical Care Records. *PNAS Nexus* 1, 4 (2022). DOI:http://dx.doi.org/10.1093/pnasnexus/pgac157

[8] Eliane Röösli, Selen Bozkurt, and Tina Hernandez-Boussard. 2022. Peeking into a black box, the fairness and generalizability of a mimic-III benchmarking model. *Scientific Data* 9, 1 (2022). DOI:http://dx.doi.org/10.1038/s41597-021-01110-7

[9] Filippo Pesapane et al. 2021. Legal and regulatory framework for AI solutions in Healthcare in EU, US, China, and Russia: New scenarios after a pandemic. *Radiation* 1, 4 (2021), 261–276. DOI:http://dx.doi.org/10.3390/radiation1040022

[10] Filippo Pesapane, Caterina Volonté, Marina Codari, and Francesco Sardanelli. 2018. Artificial Intelligence as a medical device in radiology: Ethical and regulatory issues in Europe and the United States. *Insights into Imaging* 9, 5 (2018), 745–753. DOI:http://dx.doi.org/10.1007/s13244-018-0645-y

[11] Frank Pasquale. 2015. The Secret Algorithms That Control Money and Information. *The Black Box Society* (2015). DOI:http://dx.doi.org/10.4159/harvard.9780674736061

[12] Harsh Kupwade Patil and Ravi Seshadri. 2014. Big Data Security and privacy issues in Healthcare. *2014 IEEE International Congress on Big Data* (2014). DOI:http://dx.doi.org/10.1109/bigdata.congress.2014.112

[13] Irina Brass and Andrew Mkwashi. 2022. Risk assessment and classification of medical device software for the Internet of Medical Things. *Proceedings of the 12th International Conference on the Internet of Things* (2022). DOI:http://dx.doi.org/10.1145/3567445.3571104

[14] Kerstin N. Vokinger, Thomas J. Hwang, and Aaron S. Kesselheim. 2022. Lifecycle regulation and evaluation of Artificial Intelligence and machine learning-based medical devices. *The Future of Medical Device Regulation* (2022), 13–21. DOI:http://dx.doi.org/10.1017/9781108975452.002

[15] Krishnan Ganapathy. 2021. Artificial Intelligence and Healthcare Regulatory and legal concerns. *Telehealth and Medicine Today* (2021). DOI:http://dx.doi.org/10.30953/tmt.v6.252

[16] Martin McKee and Olivier J. Wouters. 2022. The challenges of regulating artificial intelligence in healthcare comment on “Clinical decision support and new regulatory frameworks for medical devices: Are we ready for it? - a viewpoint paper.” *International Journal of Health Policy and Management* (2022). DOI:http://dx.doi.org/10.34172/ijhpm.2022.7261

[17] Michael Silva, Colleen Flood, Anna Goldenberg, and Devin Singh. 2022. Regulating the safety of health-related artificial intelligence. *Healthcare Policy | Politiques de Santé* 17, 4 (2022), 63–77. DOI:http://dx.doi.org/10.12927/hcpol.2022.26824

[18] Mohmood Alsaadi, Alexei Lisitsa, and Malik Qasaimeh. 2019. Minimizing the ambiguities in medical devices regulations based on software requirement engineering techniques. *Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems* (2019). DOI:http://dx.doi.org/10.1145/3368691.3368709

[19] Pranjal Kumar, Siddhartha Chauhan, and Lalit Kumar Awasthi. 2023. Artificial Intelligence in Healthcare: Review, Ethics, Trust Challenges & Future Research Directions. *Engineering Applications of Artificial Intelligence* 120 (2023), 105894. DOI:http://dx.doi.org/10.1016/j.engappai.2023.105894

[20] Price II, William Nicholson. 2018. Medical malpractice and black-box medicine. *Big Data, Health Law, and Bioethics*, 295–306. DOI:http://dx.doi.org/10.1017/9781108147972.027

[21] Richard Rak. 2021. Internet of healthcare: Opportunities and legal challenges in internet of things-enabled telehealth ecosystems. *14th International Conference on Theory and Practice of Electronic Governance* (2021). DOI:http://dx.doi.org/10.1145/3494193.3494260

[22] Stan Benjamens, Pranavsingh Dhunnoo, and Bertalan Meskó. 2020. The state of Artificial Intelligence-based FDA-approved Medical Devices and algorithms: An online database. *npj Digital Medicine* 3, 1 (2020). DOI:http://dx.doi.org/10.1038/s41746-020-00324-0

[23] Yoonyoung Park, Gretchen Purcell Jackson, Morgan A. Foreman, Daniel Gruen, Jianying Hu, and Amar K. Das. 2020. Evaluating Artificial Intelligence in medicine: Phases of clinical research. *JAMIA Open* 3, 3 (2020), 326–331. DOI:http://dx.doi.org/10.1093/jamiaopen/ooaa033

[24] Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan. 2019. Dissecting racial bias in an algorithm used to manage the health of populations. *Science* 366, 6464 (2019), 447–453. DOI:http://dx.doi.org/10.1126/science.aax2342