Received November 7, 2024, accepted January 6, 2025, date of publication January 15, 2025.

Review

Balancing Innovation and Safety in Digital Healthcare

Shalini Sharma[1], Maninder Singh[2,*] and Keerti Bhusan Pradhan[1]

[1] Chitkara Business School, Chitkara University Punjab, Chandigarh-Patiala National Highway, Punjab-140401, India.
[2] T A Pai Management Institute, Manipal Academy of Higher Education, Manipal-576104, India.

[*] Corresponding Author Email: maninder.singh@manipal.edu

ABSTRACT

In an era of rapid digital transformation, patient safety is increasingly intertwined with technological advancements in healthcare. This article explores the dual nature of these innovations, where tools like telemedicine, artificial intelligence (AI), and electronic health records (EHRs) offer significant potential to enhance care delivery and introduce new risks such as algorithmic bias, cybersecurity threats, and challenges in minimizing patient risks. A balanced approach focusing on robust safety protocols and continuous learning is required to ensure technology enhancement without undermining patient safety. The paper aims to advance the discourse on integrating technology with patient-centric care, proposing future research and policy development strategies to sustain a high safety standard in an increasingly digital healthcare environment.

Keywords—*Digital health, Artificial intelligence, Telemedicine, Cybersecurity, Healthcare innovation, Patient safety.*

INTRODUCTION

Integrating digital technologies into healthcare supports enhancing patient outcomes, streamlining workflows, and making healthcare more accessible. Digital tools such as Electronic Health Records (EHRs), telemedicine, and artificial intelligence (AI) offer unprecedented opportunities to enhance patient care.[1,2] While these innovations have the potential to revolutionize patient care, they also pose significant risks if their implementation outpaces patient safety protocols.[3,4]

This intersection of technological innovation and patient safety has emerged as a critical area of focus. As the healthcare sector embraces digitalization and health systems become increasingly complex, these advancements hold the potential for both groundbreaking improvements and unintended risks. The challenge lies in ensuring that these technologies are implemented in ways that prevent inadvertent harm to patients.[4]

Digitized Healthcare systems must prioritize identifying and mitigating risks associated with new technologies.[2] The adoption of digital tools like AI and telemedicine should be viewed through a lens of sustainability, where the focus should be on developing resilient healthcare systems that can adapt to and mitigate emerging risks.[1] A proactive stance in technology integration could ensure patient safety is not compromised in pursuing technological progress.[4]

The challenges associated with new technological advancement in the healthcare sector are even more complex compared to other sectors. The nature of healthcare demands is different in different geographical regions. Further, there are disparities in how technology is implemented and accessed across different regions, particularly in low- and middle-income countries. These areas often face significant challenges in adopting advanced technologies due to resource limitations, which can exacerbate existing inequalities in patient safety outcomes.[5] Therefore, the benefits of digital tools that can enhance care delivery, are not universally experienced. Technological advancements must ensure equitable distribution and safe implementation across diverse healthcare settings and geographies.[6]

To address these disparities effectively, it is essential to integrate policy and organizational culture into the safe adoption of technology within healthcare systems. Policies must be adaptable and forward-thinking, balancing the promotion of technological advancements with the imperative to safeguard patient safety.[7] Equally important is fostering an organizational culture that prioritizes safety, encourages transparency, and supports continuous learning. Such a culture not only mitigates risks associated with new technologies but also empowers healthcare professionals to engage in proactive safety practices, thereby enhancing the overall resilience of the healthcare system.[8]

A balanced approach that prioritizes both innovation and safety is essential to harness the full potential of digital health. This requires a comprehensive understanding of how technologies influence various aspects of healthcare, along with a commitment to continuous learning and adaptation. Ensuring safety protocols keep pace with technological advancements is critical to mitigating risks and maximizing benefits.[2,4] By fostering a culture of safety, we can navigate the complexities of digital health and towards the future of robust healthcare systems. This paper aims to contribute to the ongoing discourse by offering insights that will help shape the future of patient safety in the digital age.[1,9] The paper explores the dualities, emphasizing the need for a balanced approach that maximizes the benefits of technology while safeguarding the fundamental principles of patient safety.[10]

METHODS

This study utilized a systematic literature review methodology to identify, evaluate, and synthesize peer-reviewed articles relevant to the intersection of patient safety and healthcare technologies, AI, telemedicine, and cybersecurity. The selection process was guided by the expertise of two highly qualified reviewers. One reviewer from the field of patient safety has extensive experience in identifying key issues in this field. The second reviewer specializes in quality control, focusing on integrating safety principles into healthcare systems. This dual expertise ensured a high evaluation standard, significantly enhancing the quality and reliability

of the selected studies for this review.

The review process began with a comprehensive search across four major academic databases: Scopus, Web of Science, PubMed, and Google Scholar, spanning publications from January 2014 to October 2024. A carefully curated search strategy was employed, utilizing thematic keywords designed to capture diverse terminologies and contexts associated with the study's themes. Terms such as "Artificial Intelligence", "Machine Learning", "Telemedicine", "Digital Health", "Healthcare Cybersecurity", "Health Disparities", and "Patient Safety" were included. Synonyms and alternative terms were explicitly incorporated to account for variability in terminology, such as "telehealth" alongside "telemedicine" and "electronic medical records (EMR)" alongside "electronic health records (EHR)". Boolean operators (e.g., AND, OR) and phrase searching were used to refine the search, while database-specific subject headings (e.g., MeSH terms in PubMed) further enhanced precision. This approach resulted in the retrieval of 234 articles, which were subsequently imported into reference management software for de-duplication.

After removing 28 duplicate records, 206 unique articles remained for title and abstract screening. Reviewers independently evaluated the articles based on predefined inclusion and exclusion criteria during this phase. Articles were included if they were empirical, peer-reviewed studies addressing healthcare technology, AI, telemedicine, or cybersecurity, published in English, and indexed in Scopus, Web of Science, or PubMed. Articles not meeting these criteria such as theoretical papers, non-peer-reviewed studies, or those unrelated to healthcare were excluded, leaving 87 articles for full-text review.

The full-text review phase, conducted by the same domain experts, excluded an additional 45 studies due to methodological limitations, irrelevance, or insufficient indexing. This process culminated in the selection of 42 articles for inclusion in the final review. These articles represented a diverse array of topics in the context of patient safety, including AI in healthcare (12 articles), telemedicine and digital health (10 articles), cybersecurity in healthcare systems (9 articles), digital divide (8 articles), and health disparities (3 articles). Geographically, the articles spanned studies conducted in North America, Europe, Asia, and Africa, providing a global perspective on the intersection of technology and healthcare.

The quality of the selected articles was validated through their indexing in major academic databases. Of the 42 articles, 38 (90.5%) were indexed in Scopus, 34 (81%) in Web of Science, and 30 (71%) in PubMed. Notably, 28 articles (66.7%) were indexed across all three databases, underscoring their multidisciplinary relevance and high scholarly standards. This systematic review methodology, characterized by a robust search strategy, precise selection criteria, and expert oversight, ensured the inclusion of high-quality, globally relevant studies. The synthesis focused on a qualitative narrative rather than a quantitative meta-analysis due to study heterogeneity.

LITERATURE REVIEW

The Key Challenges

Persistence of Medical Errors

Despite advances in medical technology, medical errors continue to plague healthcare systems worldwide, with around 33% of patients experiencing harm during healthcare delivery.[11] Studies have shown that the incidence of adverse events among hospitalized patients remains high globally despite increased digitalization in healthcare delivery.[12–14] This trend raises concerns about the effectiveness of current patient safety strategies and the disparity in resource allocation to safety initiatives compared to other medical priorities such as technology adoption.[15,16]

Health Inequities and the Digital Divide

While technology has the potential to reduce healthcare disparities, the digital divide continues to exacerbate health inequities, particularly for vulnerable populations,[17–19] Underprivileged communities may lack access to the necessary devices or internet connectivity to utilize telemedicine and remote monitoring technologies effectively.[20,21] These gaps in access further highlight the need for comprehensive policies and investment in digital infrastructure to ensure that advancements in

healthcare technology benefit all patients, regardless of socioeconomic status.[22,23]

Challenges of Telemedicine

The advent of telemedicine, particularly accelerated during the COVID-19 pandemic, presents both opportunities and challenges in healthcare delivery. While telemedicine enhances accessibility, it also increases the risk of miscommunication and missed diagnoses due to the lack of comprehensive physical examinations.[24–26] Moreover, technological illiteracy and inadequate access to digital devices exacerbate health disparities, especially in low-resource healthcare settings.[27–29] This highlights the importance of ensuring equitable access to telehealth services and addressing the underlying social determinants that hinder the effective use of such technologies.

Remote Monitoring

Remote monitoring technologies, particularly in managing chronic illnesses, have gained traction due to their ability to provide continuous data on patient health. However, these technologies are not without risks. Delays in healthcare provider responses or misinterpretation of remote data can lead to adverse patient outcomes.[30,31] Moreover, the effectiveness of remote monitoring depends on the accuracy and timeliness of the data collected. Underscoring the need for healthcare providers to carefully evaluate these technologies before implementation.[3,31,32]

Algorithmic Bias in AI

AI in healthcare holds the potential to improve diagnostic accuracy and optimize treatment plans. However, algorithmic bias remains a significant concern, particularly when AI models are trained on datasets that lack diversity.[33–35] Such biases can lead to inaccurate diagnoses and treatment recommendations that disproportionately affect marginalized populations.[36] For example, biased AI systems have been found to suggest less aggressive treatments for black patients compared to white patients, perpetuating health inequities.[37,38] Addressing this requires both, technological advancements and ethical considerations during the development and deployment of AI in healthcare.

Risks of Overreliance on Automation

The increasing automation of healthcare processes, while reducing human error in some cases, also poses risks. Overreliance on automated systems can lead to complacency among caregivers, diminishing their clinical judgment and decision-making capabilities.[39–41] Ensuring that healthcare professionals maintain their skills and remain critical of automated recommendations is essential for patient safety.[42] The balance between automation and clinical expertise is crucial to protect the medical proficiency of healthcare providers.

Cybersecurity Vulnerabilities in Healthcare Systems

The digitalization of healthcare has also introduced cybersecurity risks, which, if not properly addressed, can jeopardize patient safety.[43–45] Cyberattacks, including ransomware, disrupt healthcare services and compromise sensitive patient data.[46] The WannaCry ransomware attack, which targeted the UK's National Health Service (NHS), highlighted the potential for widespread disruption caused by inadequate cybersecurity measures.[47–49] As healthcare organizations increasingly adopt digital tools, governments and healthcare providers must prioritize cybersecurity investments and training to protect patient data and maintain uninterrupted care delivery.[50,51]

Thus, the extant literature highlights that digital technologies in healthcare hold promise but they also come with significant risks to patient safety, particularly in vulnerable populations and low-resource settings. To fully harness these technologies' potential, addressing issues such as cybersecurity, algorithmic bias, access disparities, and overreliance on automation is imperative. Ensuring patient safety in a digitalized healthcare environment requires a coordinated effort between healthcare providers, policymakers, and technology developers to mitigate these risks while advancing the quality of care.

RECOMMENDATIONS

Solutions to These Challenges

The solution to these challenges lies in the need for a balanced approach that embraces technological advancements and addresses the associated risks.

Integrating Technology with a Patient-Centric Approach

To mitigate the risks associated with digital technologies in healthcare, a patient-centric approach must be prioritized. This approach involves designing and implementing technologies that enhance patient safety while maintaining human oversight. For instance, AI algorithms should be developed with diverse datasets to avoid biases and ensure equity in healthcare outcomes.[52–54] Additionally, involving healthcare professionals in designing and deploying these technologies can bridge the gap between technological innovation and practical and safe application.[55–57]

Enhancing Interoperability of EHR Systems

One of the significant challenges with EHRs is the lack of interoperability between different systems, which leads to incomplete patient records and potential safety risks. To address this, healthcare organizations should adopt standardized data sharing and integration protocols across platforms.[58,59] This can be supported by government policies that mandate interoperability standards, ensuring that patient data can be accurately and securely accessed regardless of the system in use. The adoption of open-source solutions has shown promise in creating more adaptable and interoperable systems.[60]

Developing Robust Cybersecurity Frameworks

Given the increasing threats of cyberattacks on healthcare systems, developing and implementing robust cybersecurity frameworks is imperative. These should include regular updates to software systems, training for healthcare staff on recognizing and responding to cyber threats, and the adoption of advanced encryption methods to protect patient data. By investing in robust security systems, healthcare organizations can protect their patient's safety and operational integrity.[61]

Continuous Education and Training for Healthcare Providers

As digital technologies evolve, continuous education and training for healthcare providers are essential. This training should focus on using new technologies effectively and understanding their limitations and potential risks.[62,63] For example, training programs could include modules on the ethical implications of AI in diagnosis and treatment, emphasizing the importance of critical thinking and human oversight in automated processes.[64–66] Continuous professional development ensures that healthcare providers remain competent and confident in the face of rapidly changing technology.

Implementing Rigorous Evaluation and Feedback Mechanisms

To ensure that new technologies are safe and effective, healthcare systems should implement rigorous evaluation and feedback mechanisms. These mechanisms should involve continuous monitoring of technology performance, patient outcomes, and user experiences. Feedback from healthcare providers and patients should be systematically collected and used to refine and improve technologies.[67,68]

Suggestions for Policy and Regulatory Framework

The successful integration of digital technologies in healthcare requires robust policy and regulatory support. Policy makers and regulatory bodies should develop comprehensive frameworks that promote innovation while ensuring patient safety.

Setting clear guidelines for the ethical use of AI, mandating regular safety audits of EHR systems, and establishing protocols for responding to cybersecurity threats. These policies should be flexible enough to adapt to the fast-paced evolution of digital health technologies while maintaining stringent safety standards.[69,70]

Policymakers must create a comprehensive regulatory framework providing clear guidelines to healthcare institutions regarding the use of AI algorithms in healthcare, and must undergo rigorous testing and validation to prevent biases that could lead to unequal treatment outcomes.[66,71]

Stringent cybersecurity standards for all healthcare institutions, including mandatory encryption protocols, regular software updates, and comprehensive training for healthcare professionals on recognizing and responding to cyber threats. Additionally, there should be a legal requirement for healthcare organizations to report cyberattacks promptly, enabling a coordinated response and minimizing the impact on patient care.[62]

Government policies should also incentivize healthcare institutions especially in low- and middle-income regions to invest in advanced cybersecurity measures, such as AI-based threat detection systems, to protect patient data and ensure operational continuity.[72]

Setting national standards for data sharing and integration, ensuring that patient information can be seamlessly transferred across healthcare providers without compromising safety. Interoperability standards should be designed to support patient privacy while allowing healthcare professionals access to comprehensive patient histories, thus reducing the likelihood of medical errors.[73]

Policies should encourage the development of open-source EHR platforms that can be easily adapted to different healthcare settings, particularly in resource-limited environments.[74]

Establishing quality assurance programs to monitor and evaluate the effectiveness of remote healthcare services. These programs should include protocols for ensuring that telemedicine consultations are conducted with the same level of care as in-person visits. This could involve the development of standardized telemedicine practices, including guidelines for when physical examinations are necessary and protocols for ensuring accurate patient assessments.[75]

Scope for Future Research

Future research could focus on understanding and mitigating the biases inherent in AI systems used in healthcare. Researchers should explore the ethical implications of AI in healthcare, examining how these technologies can be designed to promote equity in treatment outcomes across different demographic groups.

There is a critical need for longitudinal studies assessing EHR systems' long-term impact on patient safety and healthcare outcomes. Future research could investigate how EHR-related issues, such as alert fatigue and data entry errors, evolve and what their implications are for patient safety.

Future research could focus on developing innovative cybersecurity solutions tailored to the healthcare sector. This includes exploring the use of AI for real-time threat detection and response and investigating new encryption technologies that can protect patient data without hindering legitimate users' access.

Studies could evaluate the effectiveness of telemedicine across different patient populations, particularly in rural and underserved areas. This includes studying the impact of telemedicine on healthcare access, patient outcomes, and satisfaction, as well as identifying barriers to effective telemedicine use.

DISCUSSION

The review illustrates that digital health technologies hold tremendous potential to improve patient care but also pose substantial risks that require ongoing evaluation, ethical considerations, and regulatory oversight. Ensuring patient safety in the digital age demands a multi-faceted approach involving continuous education, developing robust safety protocols, and establishing policies that foster both technological innovation and equity in healthcare delivery. This discussion reaffirms the need for healthcare systems to prioritize patient safety at every stage of technological integration, ensuring that digital health's benefits are realized without compromising care quality or exacerbating disparities.

The critical examination of the intersection of technological advancements and patient safety, offering insights into both the promise and perils of digital transformation in healthcare. While digital tools such as Electronic Health Records (EHRs), telemedicine, and AI have the potential to enhance care delivery, they also introduce significant risks that must be addressed proactively. Despite advancements in digital health, the persistence of medical errors underscores the complexity of ensuring patient safety in an increasingly digitized healthcare environment.

The rise of telemedicine, accelerated by the COVID-19 pandemic, represents a paradigm shift in healthcare delivery. However, its success is contingent upon equitable access and resolving inherent limitations, such as the absence of comprehensive physical examinations and technological illiteracy among vulnerable populations. These challenges illustrate that telemedicine can exacerbate existing health inequities rather than alleviate them without careful attention to implementation and infrastructure. Therefore,

policymakers must ensure that digital health solutions are accessible, effective, and tailored to diverse populations.

The review also highlighted the significant risks posed by algorithmic bias in AI systems, which can perpetuate health disparities if not properly addressed. AI's reliance on non-representative datasets can result in biased diagnoses and treatment plans, disproportionately affecting marginalized communities. Addressing this issue requires both technological advancements and ethical oversight to ensure that AI systems are trained on diverse and inclusive datasets. Furthermore, the risks of overreliance on automation, suggest the need for healthcare providers to maintain critical thinking and clinical judgment when interacting with digital tools.

In terms of cybersecurity, the digitalization of healthcare has made systems more vulnerable to cyberattacks, which can jeopardize both patient safety and data privacy. Robust cybersecurity frameworks and regular updates to software systems are essential to safeguarding patient data and ensuring the continuity of care. Additionally, training healthcare personnel to recognize and respond to cyber threats is critical in preventing disruptions in care delivery.

The analysis of remote monitoring technologies has revealed both the advantages and challenges of these tools in managing chronic illnesses. While remote monitoring offers the ability to continuously track patient health, the reliability of the data and the timeliness of healthcare responses are critical to ensuring positive patient outcomes. Delays in addressing essential health changes can result in adverse outcomes, underscoring the importance of healthcare providers carefully evaluating these technologies before widespread implementation.

CONCLUSION

While advancements like AI, EHRs, and telemedicine offer significant potential to improve healthcare, they must be deployed with strong safety protocols, attention to equity, and comprehensive regulatory oversight. There is an urgent need for a global, future-focused commitment to patient safety in the digital era. Without these safeguards, the risks—such as algorithmic bias, cybersecurity threats, and unequal access—can undermine the very goals of improving patient outcomes. This paper suggests a cohesive, patient-centric strategy that continuously evaluates emerging technologies to ensure they enhance, rather than compromise, the quality and safety of care.

AUTHOR CONTRIBUTIONS

Conceptualization, S.S.; Methodology, S.S.; Investigation, S.S.; Writing–Original Draft Preparation, S.S.; Writing–Review & Editing, M.S. and K.B.P.; Visualization, M.S. and K.B.P.; Supervision, M.S. and K.B.P.; Project Administration, M.S. and K.B.P.

FUNDING

This research received no external funding.

DATA AVAILABILITY STATEMENT

Not required.

CONFLICTS OF INTEREST

The authors declare they have no competing interests.

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not required.

CONSENT FOR PUBLICATION

Not required.

FURTHER DISCLOSURE

Not applicable.

REFERENCES

1. Nair, M., Wen, X., Lin, X., et al. Barriers and enablers for implementation of an artificial intelligence-based decision support tool to reduce the risk of readmission of patients with heart failure: stakeholder interviews. *JMIR Form Res*. 2023;7:e47335. https://doi.org/10.2196/47335.

2. Lin, M.C.M., Kim, T.H., Kim, W.S., et al. Involvement of frontline clinicians in healthcare technology development: lessons learned from a ventilator project. *Health Technol*. 2022;12(3):597–606. https://doi.org/10.1007/s12553-022-00655-w.
3. Taylor, M.L., Thomas, E.E., Snoswell, C.L., et al. Does remote patient monitoring reduce acute care use? A systematic review. *BMJ Open*. 2021;11:e040232. https://doi.org/10.1136/bmjopen-2020-040232.
4. Gajarawala, S.N. and Pelkowski, J.N. Telehealth benefits and barriers. *J Nurse Pract*. 2021;17(2):218–221. https://doi.org/10.1016/j.nurpra.2020.09.013.
5. Kruk, M.E., Gage, A.D., Joseph, N.T., et al. Mortality due to low-quality health systems in the universal health coverage era: a systematic analysis of amenable deaths in 137 countries. *Lancet*. 2018;392:2203–2212. https://doi.org/10.1016/S0140-6736(18)31668-4.
6. Rodriguez, N.M., Burleson, G., Linnes, J.C., et al. Thinking beyond the device: an overview of human- and equity-centered approaches for health technology design. *Annu Rev Biomed Eng*. 2023;25:257–280. https://doi.org/10.1146/annurev-bioeng-081922-024834.
7. Isherwood, P. and Waterson, P. To err is system; a comparison of methodologies for the investigation of adverse outcomes in healthcare. *J Patient Saf Risk Manag*. 2021;26(2):64–73. https://doi.org/10.1177/2516043521990261.
8. Sharifian, R., Ghasemi, S., Kharazmi, E., et al. An evaluation of the risk factors associated with implementing projects of health information technology by fuzzy combined ANP-DEMATEL. *PLoS One*. 2023;18(2):e0279819. https://doi.org/10.1371/journal.pone.0279819.
9. Topol, E.J. High-performance medicine: the convergence of human and artificial intelligence. *Nat Med*. 2019;25(1):44–56. https://doi.org/10.1038/s41591-018-0300-7.
10. Crigger, E., Reinbold, K., Hanson, C., et al. Trustworthy augmented intelligence in health care. *J Med Syst*. 2022;46(2):12. https://doi.org/10.1007/s10916-021-01790-z.
11. Hodkinson, A., Tyler, N., Ashcroft, D.M., et al. Preventable medication harm across health care settings: a systematic review and meta-analysis. *BMC Med*. 2020;18(1):313. https://doi.org/10.1186/s12916-020-01774-9.
12. Klein, D.O., Rennenberg, R.J.M.W., Koopmans, R.P., et al. A systematic review of methods for medical record analysis to detect adverse events in hospitalized patients. *J Patient Saf*. 2021;17(8):e1234-e1240. https://doi.org/10.1097/PTS.0000000000000670.
13. Sauro, K.M., Machan, K.M., Whalen-Browne, L., et al. Evolving factors in hospital safety: a systematic review and meta-analysis of hospital adverse events. *J Patient Saf*. 2021;17. https://doi.org/10.1097/PTS.0000000000000889.
14. Vasudevan, A., Plombon, S., Piniella, N., et al. Effect of digital tools to promote hospital quality and safety on adverse events after discharge. *J Am Med Inform Assoc*. 2024;31(10):2304–2314. https://doi.org/10.1093/jamia/ocae176.
15. Subbe, C.P., Tellier, G., Barach, P. Impact of electronic health records on predefined safety outcomes in patients admitted to hospital: a scoping review. *BMJ Open*. 2021;11(1):e047446. https://doi.org/10.1136/bmjopen-2020-047446.
16. Vikan, M., Haugen, A.S., Bjørnnes, A.K., et al. The association between patient safety culture and adverse events: a scoping review. *BMC Health Serv Res*. 2023;23(1):300. https://doi.org/10.1186/s12913-023-09332-8.
17. Hadjiat, Y. Healthcare inequity and digital health—a bridge for the divide, or further erosion of the chasm? *PLoS Digit Health*. 2023;2(6):e0000268. https://doi.org/10.1371/journal.pdig.0000268.
18. Eruchalu, C.N., Pichardo, M.S., Bharadwaj, M., et al. The expanding digital divide: digital health access inequities during the COVID-19 pandemic in New York City. *J Urban Health*. 2021;98(2):183–186. https://doi.org/10.1007/s11524-020-00508-9.
19. Spanakis, P., Peckham, E., Mathers, A., et al. The digital divide: amplifying health inequalities for people with severe mental illness in the time of COVID-19. *Br J Psychiatry*. 2021;219(4):529–531. https://doi.org/10.1192/bjp.2021.56.

20. Rodriguez, J.A., Betancourt, J.R., Sequist, T.D., et al. Differences in the use of telephone and video telemedicine visits during the COVID-19 pandemic. *Am J Manag Care*. 2021;27(1):21–26. https://doi.org/10.37765/ajmc.2021.88573.

21. Daniels, B., McGinnis, C., Topaz, L.S., et al. Bridging the digital health divide—patient experiences with mobile integrated health and facilitated telehealth by community-level indicators of health disparity. *J Am Med Inform Assoc*. 2024;31(4):875–883. https://doi.org/10.1093/jamia/ocae007.

22. Clare, C.A. Telehealth and the digital divide as a social determinant of health during the COVID-19 pandemic. *Netw Model Anal Health Inform Bioinform*. 2021;10(1):26. https://doi.org/10.1007/s13721-021-00300-y.

23. Jerjes, W. and Harding, D. Telemedicine in the post-COVID era: balancing accessibility, equity, and sustainability in primary healthcare. *Front Digit Health*. 2024;6:1432871. https://doi.org/10.3389/fdgth.2024.1432871.

24. Hollander, J.E. and Carr, B.G. Virtually perfect? Telemedicine for COVID-19. *N Engl J Med*. 2020;382(18):1679–1681. https://doi.org/10.1056/NEJMp2003539.

25. Bashshur, R., Doarn, C.R., Frenk, J.M., et al. Telemedicine and the COVID-19 pandemic, lessons for the future. *Telemed J E Health*. 2020;26(5):571–573. https://doi.org/10.1089/tmj.2020.29040.rb.

26. De Simone, S., Franco, M., Servillo, G., et al. Implementations and strategies of telehealth during COVID-19 outbreak: a systematic review. *BMC Health Serv Res*. 2022;22(1):833. https://doi.org/10.1186/s12913-022-08235-4.

27. Mee, P., Gussy, M., Huntley, P., et al. Digital exclusion as a barrier to accessing healthcare: a summary composite indicator and online tool to explore and quantify local differences in levels of exclusion. *Univers Access Inf Soc*. 2024. https://doi.org/10.1007/s10209-024-01148-5.

28. Paik, K.E., Hicklen, R., Kaggwa, F., et al. Digital determinants of health: health data poverty amplifies existing health disparities—a scoping review. *PLOS Digit Health*. 2023;2(10):e0000313. https://doi.org/10.1371/journal.pdig.0000313.

29. Bentley, S.V., Naughtin, C.K., McGrath, M.J., et al. The digital divide in action: how experiences of digital technology shape future relationships with artificial intelligence. *AI Ethics*. 2024;4(4):901–915. https://doi.org/10.1007/s43681-024-00452-3.

30. Liu, J.C., Cheng, C.Y., Cheng, T.H., et al. Unveiling the potential: remote monitoring and telemedicine in shaping the future of heart failure management. *Life*. 2024;14(8):936. https://doi.org/10.3390/life14080936.

31. Ekstedt, M., Nordheim, E.S., Hellström, A., et al. Patient safety and sense of security when telemonitoring chronic conditions at home: the views of patients and healthcare professionals—a qualitative study. *BMC Health Serv Res*. 2023;23(1):581. https://doi.org/10.1186/s12913-023-09428-1.

32. Hilty, D.M., Armstrong, C.M., Edwards-Stewart, A., et al. Sensor, wearable, and remote patient monitoring competencies for clinical care and training: scoping review. *J Technol Behav Sci*. 2021;6(2):252–277. https://doi.org/10.1007/s41347-020-00190-3.

33. Panch, T., Mattie, H., Atun, R. Artificial intelligence and algorithmic bias: implications for health systems. *J Glob Health*. 2019;9(2):020318. https://doi.org/10.7189/jogh.09.020318.

34. Seyyed-Kalantari, L., Zhang, H., McDermott, M.B.A., et al. Underdiagnosis bias of artificial intelligence algorithms applied to chest radiographs in underserved patient populations. *Nat Med*. 2021;27(12):2176–2182. https://doi.org/10.1038/s41591-021-01595-0.

35. Ghassemi, M., Oakden-Rayner, L., Beam, A.L. The false hope of current approaches to explainable artificial intelligence in health care. *Lancet Digit Health*. 2021;3(11):e745–e750. https://doi.org/10.1016/S2589-7500(21)00208-9.

36. Celi, L.A., Cellini, J., Charpignon, M.L., et al. Sources of bias in artificial intelligence that perpetuate healthcare disparities—A global review. *PLOS Digit Health*. 2022;1(3):e0000022. https://doi.org/10.1371/journal.pdig.0000022.

37. Obermeyer, Z., Powers, B., Vogeli, C., et al. Dissecting racial bias in an algorithm used to manage the health of populations. *Science*. 2019;366(6464):447–453. https://doi.org/10.1126/science.aax2342.

38. Vyas, D.A., Eisenstein, L.G., Jones, D.S. Hidden in plain sight—reconsidering the use of race correction in clinical algorithms. *N Engl J Med*. 2020;383(9):874–882. https://doi.org/10.1056/NEJMms2004740.

39. Khera, R., Simon, M.A., Ross, J.S. Automation bias and assistive AI: risk of harm from AI-driven clinical decision support. *JAMA*. 2023;330(23):2255–2257. https://doi.org/10.1001/jama.2023.22557.

40. Alanazi, A. Clinicians' views on using artificial intelligence in healthcare: opportunities, challenges, and beyond. *Cureus*. 2023;15(9):e45255. https://doi.org/10.7759/cureus.45255.

41. Abdelwanis, M., Alarafati, H.K., Tammam, M.M.S., et al. Exploring the risks of automation bias in healthcare artificial intelligence applications: A Bowtie analysis. J. *Saf. Sci. Resil*. 2024;5(4):460–469. https://doi.org/10.1016/j.jnlssr.2024.06.001.

42. Ratwani, R.M., Bates, D.W., Classen, D.C. Patient safety and artificial intelligence in clinical care. *JAMA Health Forum*. 2024;5(2):e235514. https://doi.org/10.1001/jamahealthforum.2023.5514.

43. Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., et al. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC Med Inform Decis Mak*. 2020;20(1):146. https://doi.org/10.1186/s12911-020-01161-7.

44. Neprash, H.T., McGlave, C.C., Cross, D.A., et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum*. 2022;3(12):e224873. https://doi.org/10.1001/jamahealthforum.2022.4873.

45. Mejía-Granda, C.M., Fernández-Alemán, J.L., Carrillo-de-Gea, J.M., et al. Security vulnerabilities in healthcare: an analysis of medical devices and software. *Med Biol Eng Comput*. 2024;62(1):257–273. https://doi.org/10.1007/s11517-023-02912-0.

46. Nemec Zlatolas, L., Welzer, T., Lhotska, L. Data breaches in healthcare: security mechanisms for attack mitigation. *Clust. Comput*. 2024;27(7):8639–8654. https://doi.org/10.1007/s10586-024-04507-2.

47. Investigation: WannaCry cyber attack and the NHS. Available online: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

48. Ghafur, S., Grass, E., Jennings, N.R., et al. The challenges of cybersecurity in health care: the UK National Health Service as a case study. *Lancet Digit Health*. 2019;1(1):e10–e12. https://doi.org/10.1016/S2589-7500(19)30005-6.

49. Ghafur, S., Kristensen, S., Honeyford, K., et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digit Med*. 2019;2:98. https://doi.org/10.1038/s41746-019-0161-6.

50. Frati, F., Darau, G., Salamanos, N., et al. Cybersecurity training and healthcare: the AERAS approach. *Int. J. Inf. Secur*. 2024;23:1527–1539. https://doi.org/10.1007/s10207-023-00802-y.

51. Tomlinson, E.W., Abrha, W.D, Kim, S.D., et al. Cybersecurity access control: framework analysis in a healthcare institution. *J Cybersecur Priv*. 2024;4(3):762–776. https://doi.org/10.3390/jcp4030035.

52. Yang, J., Soltan, A.A., Eyre, D.W., et al. An adversarial training framework for mitigating algorithmic biases in clinical machine learning. *NPJ Digit Med*. 2023;6(1):55. https://doi.org/10.1038/s41746-023-00805-y.

53. Abràmoff, M.D., Tarver, M.E., Loyo-Berrios, N., et al. Considerations for addressing bias in artificial intelligence for health equity. *NPJ Digit Med*. 2023;6(1):170. https://doi.org/10.1038/s41746-023-00913-9.

54. Ritoré, Á., Jiménez, C.M., González, J.L., et al. The role of open access data in democratizing healthcare AI: a pathway to research enhancement, patient well-being, and treatment equity in Andalusia, Spain. *PLOS Digit Health*. 2024;3(9):e0000599. https://doi.org/10.1371/journal.pdig.0000599.

55. Bird, M., McGillion, M., Chambers, E.M., et al. A generative co-design framework for healthcare innovation: development and application of an end-user engagement framework. *Res Involv Engagem*. 2021;7(1):1–12. https://doi.org/10.1186/s40900-021-00252-7.

56. Holden, R.J., Boustani, M.A., Azar, J. Agile innovation to transform healthcare: innovating in complex adaptive systems is an everyday process, not a light bulb event. *BMJ Innov*. 2021;7(1):399–505. https://doi.org/10.1136/bmjinnov-2020-000574.

57. Liao, F., Adelaine, S., Afshar, M., et al. Governance of clinical AI applications to facilitate safe and equitable deployment in a large health system: key elements and early successes. *Front Digit Health*. 2022;4:931439. https://doi.org/10.3389/fdgth.2022.931439.

58. Benson, T. and Grieve, G. *Principles of health interoperability*. Springer: Cham, Switzerland; 2021; pp. 21–40. https://doi.org/10.1007/978-3-030-56883-2.

59. Li, E., Clarke, J., Ashrafian, H., et al. The impact of electronic health record interoperability on safety and quality of care in high-income countries: systematic review. *J Med Internet Res*. 2022;24(9):e38144. https://doi.org/10.2196/38144.

60. Turbow, S., Hollberg, J.R., Ali, M.K. Electronic health record interoperability: how did we get here and how do we move forward? *JAMA Health Forum*. 2021;2(3):e210253. https://doi.org/10.1001/jamahealthforum.2021.0253.

61. Prabha, P.D., Kumar, N.S., Shree N.N., et al. Cybersecurity in healthcare: safeguarding patient data. In *Proceedings of the 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, Chennai, India, 9–10 May 2024; IEEE: New York, USA; 2024; pp.1–6. https://doi.org/10.1109/ACCAI61061.2024.10602188.

62. Bhuyan, S.S., Kabir, U.Y., Escareno, J.M., et al. Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *J Med Syst*. 2020;44(1):1–9. https://doi.org/10.1007/s10916-019-1507-y.

63. Boutros, P., Kassem, N., Nieder, J. et al. Education and training adaptations for health workers during the COVID-19 pandemic: a scoping review of lessons learned and innovations. *Healthcare*. 2023;11(21):2902. https://doi.org/10.3390/healthcare11212902.

64. Li, F., Ruijs. N., Lu, Y. Ethics & AI: a systematic review on ethical concerns and related strategies for designing with AI in healthcare. *AI*. 2022;4(1):28-53. https://doi.org/10.3390/ai4010003.

65. Tahri-Sqalli M., Aslonov, B., Gafurov, M., et al. Humanizing AI in medical training: ethical framework for responsible design. *Front Artif Intell*. 2023;6:1189914. https://doi.org/10.3389/frai.2023.1189914.

66. Ueda, D., Kakinuma, T., Fujita, S., et al. Fairness of artificial intelligence in healthcare: review and recommendations. *Jpn J Radiol*. 2024;42(1):3–15. https://doi.org/10.1007/s11604-023-01474-3.

67. Foy, R., Skrypak, M., Alderson, S., et al. Revitalising audit and feedback to improve patient care. *BMJ*. 2020;368:m213. https://doi.org/10.1136/bmj.m213.

68. Boehnke, J.R. and Rutherford, C. Using feedback tools to enhance the quality and experience of care. *Qual Life Res*. 2021;30(11):3007–3013. https://doi.org/10.1007/s11136-021-03008-8.

69. Sittig D.F., Sengstack P., Singh H. Guidelines for US hospitals and clinicians on assessment of electronic health record safety using SAFER guides. *JAMA*. 2022;327(8):719–720. https://doi.org/10.1001/jama.2022.0085.

70. Mökander, J. Auditing of AI: legal, ethical and technical approaches. *Digit Soc*. 2023;2:49. https://doi.org/10.1007/s44206-023-00074-y.

71. Ayers, J.W., Desai, N., Smith, D.M. Regulate artificial intelligence in health care by prioritizing patient outcomes. *JAMA*. 2024;331(8):639–640. https://doi.org/10.1001/jama.2024.0549.

72. Alami, H., Rivard, L., Lehoux, P., et al. Artificial intelligence in health care: laying the foundation for responsible, sustainable, and inclusive innovation in low- and middle-income countries. *Glob Health*. 2020;16(1):52. https://doi.org/10.1186/s12992-020-00584-1.

73. Torab-Miandoab, A., Samad-Soltani, T., Jodati, A., et al. Interoperability of heterogeneous health information systems: a systematic literature review. *BMC Med Inform Decis Mak*. 2023;23(1):18. https://doi.org/10.1186/s12911-023-02115-5.

74. Brotherton, T., Brotherton, S., Ashworth, H., et al. Development of an offline, open-source, electronic health record system for refugee care. *Front Digit Health*. 2022;4:847002. https://doi.org/10.3389/fdgth.2022.847002.

75. Antoniotti, N.M. Standards and guidelines in telehealth: creating a compliance and evidence-based telehealth practice. In *Telemedicine, Telehealth and Telepresence: Principles, Strategies, Applications, and New Directions*; Latifi, R., Doarn, C.R., Merrell, R.C., eds. Springer: Cham, Switzerland; 2021; pp. 97–113. https://doi.org/10.1007/978-3-030-56917-4_7.