Navigating Ethical Challenges of Multi-Omics and Electronic Health Records in Healthcare

Atharv Joshi[1], Spruha Joshi[2], and Alireza Izadian Bidgol[3]

[1] Western University, Canada
[2] McMaster University, Canada
[3]American University of the Caribbean School of Medicine

The integration of multi-omics approaches with Electronic Health Records (EHRs) has the potential to transform personalized medicine by offering deeper insights into disease mechanisms, treatment responses, and patient outcomes. Multi-omics enhances diagnostic accuracy, treatment, optimization, and predictive modelling through the like of genomics, proteomics, and other omic layers. However, this advancement also raises critical ethical concerns regarding privacy, confidentiality, autonomy, and justice. Multi-omics data serves as a distinct biological identifier, making it highly sensitive and vulnerable to misuse. Equity in multi-omics research is another significant challenge; genomic studies have historically been biased toward populations of European descent, limiting the generalizability of findings across diverse groups. While federal regulations such as the United States' Health Insurance Portability and Accountability Act (HIPAA) and the province of Ontario's Personal Health Information Protection Act (PHIPA) establish a baseline for legal protections, their effectiveness depends on robust digital infrastructure, public education, and the development of privacy frameworks. Robust security measures such as encryption, blockchain, and privacy-preserving algorithms are essential to mitigate risks. However, existing governance frameworks must extend beyond security protocols to establish clear regulations on data ownership, access rights, and ethical usage. Emerging challenges, including AI-driven data analysis and the commercialization of genetic information, further underscore the need for proactive governance to prevent misuse, discrimination, and bias in healthcare and insurance industries. To ensure ethical multi-omics integration into EHRs, continuous policy updates, interdisciplinary collaboration, and patient-centered approaches are essential. Balancing innovation with ethical integrity will be crucial in advancing precision medicine while safeguarding individual rights and promoting equitable healthcare access.

Keywords: Ethics, Electronic Medical Records, Multi-Omics, Precision Medicine, Blockchain Technology

Introduction

Integrating multi-omics approaches with Electronic Health Records (EHRs) offers a powerful opportunity to advance personalized medicine by delivering deeper insights into disease mechanisms, treatment responses, and patient outcomes. EHRs, which contain comprehensive clinical data on a patient's medical history, treatments, and outcomes, have significantly transformed the healthcare system since their introduction in the 1960s.[1] They have revolutionized the way patient information is recorded, stored, and accessed, which has enabled faster, more accurate documentation, and improved the coordination of care.[2] All healthcare providers who are involved in the patient's medical care can now access a patient's complete medical history in real time, leading to more informed decision-making, reduced medical errors, and enhanced patient safety. Multi-omics, which emerged in the early 2000s, further reshaped healthcare by integrating data from genomics, proteomics, metabolomics, and other omics layers.[2] Genomics focuses on the study of genomes, while proteomics investigates the structure, function, and interactions of proteins. Other omics layers, such as metabolomics, transcriptomics, and epigenomics, build on genomics and proteomics to offer a more comprehensive understanding of biological processes. While each discipline provides unique molecular insights, their integration enhances the precision and personalization of healthcare, enabling physicians to diagnose diseases more accurately, predict treatment responses, and identify novel therapeutic targets.[3]

https://doi.org/10.29173/hsi497
Received 28 March 2025
Accepted 1 July 2025

Multi-omics evolved from interdisciplinary research, particularly following the completion of the Human Genome Project in 2003, and gained significant traction in 2023-2024 for its potential to advance disease prevention and manage conditions like cancer, neurological disorders, and metabolic diseases.[4,5] Multi-omics data uncovers complex biological networks, revealing how genes, proteins, metabolites, and other molecules interact to influence health and disease.[6] This systems-level understanding provides a holistic approach, improving clinical decision-making by considering not only genetic information but also environmental influences, lifestyle choices, and molecular interactions. The combination of multi-omics and EHRs offers transformative potential for healthcare, but this integration also presents critical ethical dilemmas that must be addressed before it can be fully embraced. It should be noted that many of the findings and analysis are presented from an Ontarian perspective, rather than a global one. This commentary will explore some of the ethical issues including privacy, confidentiality, autonomy, and justice.

Privacy

Privacy in ethics pertains to the control over personal information, which requires careful collection, storage, and use to maintain ethical standards and patient trust. While multi-omics advances precision medicine by identifying inherited traits, disease risks, and treatment responses, it also introduces significant privacy risks if mismanaged.[5]

A major concern is that genomic data acts as a personalized "fingerprint", revealing extensive details about an individual's health deviations, disease risks, and lineage.[7,8] The interdisciplinary nature of multi-omics necessitates extensive data sharing, making it harder to track data destinations and increasing the risk of unauthorized access.[5] Furthermore, the extensive data demands of personalized medicine heighten the risk of exposing sensitive information through seemingly unrelated samples that may be pieced together with malicious intent by insurers or employers, for example, without the individuals consent.[7,9] This is particularly critical in genetic testing, where data shared with third parties raises privacy concerns. Such vulnerabilities (weaknesses or risks in systems and practices used to manage and protect sensitive data) underscore the need for clear data retention policies and secure disposal practices.[7,9] Without such measures, these disadvantages may undermine public trust and hinder the advancement of multi-omics in EHRs and precision medicine.

To address these concerns, the current literature recommends implementing activity traceability methods (systems that monitor and log the accessibility of data), blockchain technology, and adherence to General Data Protection Regulation (GDPR) standards.[5,7] The GDPR is a legal framework enacted by the European Union in 2018 that sets strict guidelines on how personal data is collected, stored, processed, and shared. Blockchain, in particular, provides a secure framework for data sharing and verification.[5] Molla et al. propose a multi-faceted strategy to mitigate potential risks which includes strong encryption, routine security audits, stringent access controls, and clearly defined data retention policies that outline specific storage timelines, deletion criteria, and secure disposal procedures.[7] Ultimately, the integration of multi-omics data into EHRs demands a careful balance between privacy protection and data accessibility to ensure ethical use and sustain public trust in precision medicine. This balance inevitably raises critical ethical considerations, particularly surrounding patient confidentiality and autonomy, as individuals must retain control over how their sensitive health information is accessed and used.

Confidentiality and Autonomy

While confidentiality and privacy are often used interchangeably in healthcare data security, confidentiality specifically refers to the duty of safeguarding sensitive information from unauthorized disclosure, particularly in EHRs, which consolidate long-term records from multiple providers.[10]

Incorporating multi-omics data into EHRs increases security risks, as even anonymized genetic information can potentially be reidentified when combined with phenotypic or clinical data, thereby heightening the risk of data breaches.[11] Genomic data predicts individual health outcomes and inherited conditions, creating an ethical dilemma between balancing patient confidentiality while being obligated to inform relatives of genetic risks.[12]

To safeguard confidentiality, Jamshed et al. emphasize restricting EHR access through role-based permissions and traceability measures, such as user identifications and passwords for accountability.[13] Another approach in some countries is granting patients greater control over records and limiting third-party access.[10] While this enhances autonomy, it may also restrict providers' access to critical information, potentially affecting care quality.[10]

Autonomy in ethics refers to an individual's right to self-determination and informed decision-making.[14] In EHRs, clear consent frameworks are essential to ensure individuals understand how confidentiality is maintained.[8] Empowering patients to make informed choices about data sharing can bring tangible benefits, allowing healthcare to be more personalized, timely, and effective. For instance, sharing genomic information can help healthcare providers detect risks earlier and reduce trial-and-error in treatment plans. While poorly designed regulations may create a false sense of security and shift accountability away from data stewards, reducing transparency, overly rigid policies that discourage data sharing can deny patients these advancements.[15]

A well-balanced system is needed with the use of EHRs, and multi-omics to ensure sensitive information is used transparently, empowering patients to make autonomous healthcare decisions. While research on autonomy in multi-omics and EHRs remains limited, upholding individual choice is essential to maintaining ethical integrity in this advancing field.

Justice and Multi-Omics

In ethics, justice is the "fair, equitable and appropriate treatment of persons".[16] In the context of multi-omics and EHRs, justice ensures that advanced healthcare technologies benefit all populations equitably, without discrimination.[17] While multi-omics enables personalized treatments, concerns regarding access, representation, and health outcomes are persistent.

Williams and Anderson emphasize that equitable research selection is crucial, as underrepresentation limits certain groups from benefiting from scientific advancements.[17] Historically, genome-wide association studies have predominantly focused on individuals of European ancestry, creating disparities in genetic research. For instance, American biobank recruitment materials aimed at engaging Hispanic individuals were only available in English and exceeded recommended reading levels, creating barriers to participation.[17,18] This is not due to a lack of willingness but rather ineffective recruitment strategies that fail to promote inclusivity. Clarke and van El highlight that disadvantaged individuals must first receive adequate healthcare access before benefitting from genomic services.[19] Barriers such as poverty, disability, and limited internet access hinder engagement with genomic technologies.[19] Even when individuals access genomic services, they may struggle to stay informed due to changing personal circumstances or evolving genetic interpretations that impact their healthcare decisions.

Sustained access requires public initiatives and dedicated healthcare efforts to keep all patients, including those facing financial hardship, connected to the healthcare system. Achieving justice in multi-omics requires intentional efforts to improve inclusivity and equitable access. Without proactive measures, personalized medicine and EHR risks are deepening health disparities rather than reducing them.

Discussion

Researchers agree that while multi-omics and EHRs hold significant potential for precision medicine, critical issues must be addressed before integration into routine healthcare. EHRs improve healthcare quality at a relatively low cost, yet concerns persist around responsibility, data privacy, and ethical implications.[20]
A key issue is ensuring clearer consent processes, so patients fully understand how their data is used. Strong security measures are crucial to protect patient data and prevent breaches. Alongside these measures, clear guidelines on data ownership and access are essential. In North America, federal laws like the Health Insurance Portability and Accountability Act (HIPAA) in the United States and provincial laws such as Ontario's Personal Health Information Protection Act (PHIPA) provide frameworks for EHR security through access controls, encryption, and audit trails.[21] Regulatory frameworks alone are not enough, and practical implementation requires investment in secure digital health infrastructure. In Canada, Health Infoway, a federally funded agency, plays a key role in advancing secure and interoperable EHR systems to align with privacy laws. Its' ACCESS 2022 initiative aims to expand digital health services and improve patient access to their medical records while promoting data security and interoperability.[22] However, challenges remain in balancing accessibility with privacy, particularly under Ontario's Freedom of Information and Protection of Privacy Act (FIPPA).[23] While PHIPA protects personal health information,

administrative and operational hospital records containing anonymized patient data, this information may still be accessible under FIPPA.[23] FIPPA's potential to permit access to such data creates uncertainty about unintended secondary usage, emphasizing the need for updated policies that account for the sensitivity of omics data.

To further mitigate these risks, advanced security measures are essential to protect EHRs from breaches and cyber threats. Literature shows that the most effective methods for securing EHRs include encryption, firewalls, blockchain, access controls, and audit logs. Cryptogenic techniques enable selective data removal from cloud servers while maintaining privacy through encryption monitoring, digital signatures, and robust authentication.[20,24] Users should regularly update passwords, avoid weak credentials, and log out after sessions.[20] Firewall technology plays a crucial role in blocking unauthorized intranet access, while innovative methods like privacy-preserving algorithms and machine learning anonymization strengthen security against cyberattacks.[25,26] As Canada continues to expand digital health initiatives, integrating these advanced security measures will be critical to ensuring patient data remains protected while enabling multi-omics integration into healthcare.

Clear governance is equally as important to security measures in defining who has access to sensitive patient data and under what circumstances. Ethical multi-omics use requires unity, collaboration, and accountability. While governments must establish and enforce clear regulations, the ultimate responsibility rests with hospitals and research institutions to apply ethical practices in real-world settings. A major challenge is ensuring all stakeholders understand privacy obligations.[24] Tardif notes that misinterpretations of privacy laws often lead to patient consent violations in EHR access, particularly when healthcare professionals assume broad access rights beyond their intended scope, highlighting the need for better education on privacy regulations.[27]

Beyond compliance, scientists and healthcare providers must advocate for ethical standards and educate patients about their rights. For instance, academic researchers must follow Tri-Council guidelines and require certification before conducting studies.[28] The Tri-Council refers to the Tri-Council Policy Statement (TCPS) in Canada, which is a set of ethical guidelines for research involving humans. The guidelines emphasize the importance of respecting the rights, dignity, and autonomy of research participants and ensuring informed consent, privacy protection, and proper ethics review processes. Similarly in Ontario, private-sector organizations like clinics, pharmacies, and insurers are governed by the Personal Information Protection and Electronic Documents Act (PIPEDA), which regulates the collection and disclosure of personal health information.[29] Ethical concerns grow with secondary multi-omics data use in population health research and historical studies.[24] Private vendors like Google and Microsoft offer personal health records services directly to patients, but the level of security and privacy vary.[24] Without consistent oversight, privacy risks increase. A standardized privacy framework is needed to promote collaboration while protecting individual rights.[24]

As multi-omics evolves, emerging challenges require attention, particularly in AI-driven data analysis, which raises concerns about bias, accuracy, and privacy. The commercialization of genetic information presents ethical risks, including potential misuse. AI systems may fail to fully anonymize health data, use information for unintended purposes, or enable cross-border transfers that bypass regulations.[30] Predictive health data could also be exploited by insurers or employers, leading to discrimination. McGraw and Mandl highlight how social determinants of health influence wellness, making multi-omics data particularly sensitive due to stigma and financial risks.[31] For example, insurers could use this data to deny coverage to high-risk populations.[31] However, if ethically managed, AI and commercialization can expand access to care by reducing diagnostic delays and identifying patterns across underrepresented populations. If AI is used responsibly, it can be beneficial in reducing the ongoing healthcare and economic burden. To prevent ethical breaches, organizations must comply with laws like PIPEDA and implement responsible data use strategies. Privacy Incident Management Processes can help detect, mitigate, and report ethical violations.[32] Addressing these challenges requires continuous policy updates, open discussions on ethics, and adaptable regulations. Prioritizing ethical considerations will ensure multi-omics advances equitably and responsibly. It is important to understand that ultimately the role of trust in healthcare, from both patient and provider perspectives is crucial for informed consent and responsible data use.

Conclusion

This paper examined the ethical challenges associated with integrating multi-omics into EHRs and precision medicine. It explored key strengths, limitations, and existing strategies for ensuring ethical and fair use of these technologies. However, the findings are not exhaustive, as the level of ethical integration varies across healthcare facilities. Future research should focus on how multi-omics can inform clinical practice across disciplines and assess its long-term impact on patient care. Additionally, clearer consent models are needed to empower patients in making informed decisions about data usage while ensuring healthcare providers have access to essential information for optimal care.

References

1. Atherton J. Development of the Electronic Health Record. AMA Journal of Ethics [Internet]. 2011;13(3):186–9. Available from: https://journalofethics.ama-assn.org/article/development-electronic-health-record/2011-03
2. McColl ER, Asthana R, Paine MF, Piquette-Miller M. The Age of Omics-Driven Precision Medicine. Clinical Pharmacology & Therapeutics. 2019 Aug 13;106(3):477–81.
3. M. Madan Babu, Snyder M. Multi-Omics Profiling for Health. Molecular & Cellular Proteomics. 2023 Jun 1;22(6):100561–1.
4. Green ED, Guyer MS. Charting a course for genomic medicine from base pairs to bedside. Nature. 2011 Feb;470(7333):204–13.
5. Mohr AE, Ortega-Santos CP, Whisner CM, Klein-Seetharaman J, Paniz Jasbi. Navigating Challenges and Opportunities in Multi-Omics Integration for Personalized Healthcare. Biomedicines. 2024 Jul 5;12(7):1496–6.
6. Picard M, Scott-Boyer MP, Bodein A, Périn O, Droit A. Integration strategies of multi-omics data for machine learning analysis. Computational and Structural Biotechnology Journal. 2021;19:3735–46.
7. Molla G, Bitew M. Revolutionizing Personalized Medicine: Synergy with Multi-Omics Data Generation, Main Hurdles, and Future Perspectives. Biomedicines [Internet]. 2024 Nov 30;12(12):2750. Available from: https://www.mdpi.com/2227-9059/12/12/2750
8. Bonomi L, Huang Y, Ohno-Machado L. Privacy Challenges and Research Opportunities for Genomic Data Sharing. Nature Genetics. 2020 Jul 1;52(7):646–54.
9. Safarlou CW, Bredenoord AL, Vermeulen R, Jongsma KR. Scrutinizing Privacy in Multi-Omics Research: How to Provide Ethical Grounding for the Identification of Privacy-Relevant Data Properties. The American Journal of Bioethics. 2021 Nov 22;21(12):73–5.
10. Brothers KB, Rothstein MA. Ethical, legal and social implications of incorporating personalized medicine into healthcare. Personalized Medicine [Internet]. 2015 Jan;12(1):43–51. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4296905/
11. Institute of Medicine (US). Integrating Large-Scale Genomic Information into Clinical Practice: Workshop Summary [Internet]. PubMed. Washington (DC): National Academies Press (US); 2012. Available from: https://pubmed.ncbi.nlm.nih.gov/22514815/
12. Royal College of Physicians, Royal College of Pathologists and British Society for Genetic Medicine. Consent and confidentiality in genomic medicine: Guidance on the use of genetic and genomic information in the clinic. [Internet]. Report of the Joint Committee on Genomics in Medicine. London: RCP, RCPath and BSGM. 2019. Available from: https://www.rcpath.org/static/d3956d4a-319e-47ca-8ece8a122949e701/Consent-and-confidentiality-in-genomic-medicine-July-2019.pdf
13. Jamshed N, Ozair FF, Sharma A, Aggarwal P. Ethical issues in electronic health records: A general overview. Perspectives in Clinical Research. 2018;6(2):73–6.
14. Varelius J. The value of autonomy in medical ethics. Medicine, Health Care and Philosophy. 2006 Oct 11;9(3):377–88.
15. Horton R, Lucassen A. Ethical Considerations in Research with Genomic Data. The New Bioethics. 2022 Apr 28;29(1):1–15.
16. Varkey B. Principles of clinical ethics and their application to practice. Medical Principles and Practice [Internet]. 2020 Jun 4;30(1):17–28. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC7923912/
17. Williams JK, Anderson CM. Omics research ethics considerations. Nursing Outlook. 2018 Jul;66(4):386–93.
18. Cohn EG, Henderson GE, Appelbaum PS. Distributive justice, diversity, and inclusion in precision medicine: what will success look like? Genetics in Medicine. 2016 Aug 4;19(2):157–9.
19. Clarke AJ, van El CG. Genomics and justice: mitigating the potential harms and inequities that arise from the implementation of genomics in medicine. Human Genetics. 2022 Apr 12;141(5):1099–107.
20. Basil N, Ambe S, Ekhator C, Fonkem E. Health records database and inherent security concerns: A review of the literature [Internet]. Nih.gov. 2024. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9647912/
21. Department of Health & Human Services USA. OFFICE RIGHTS FOR CIVIL Privacy, Security, and Electronic Health Records 1 PRIVACY, SECURITY, AND ELECTRONIC HEALTH RECORDS [Internet]. hhs.gov. 2013. Available from: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf
22. Neumeier M. Access 2022: Setting New Goals for Digital Health in Canada. Canadian Journal of Nursing Informatics [Internet]. 2019;14(1). Available from: https://www.proquest.com/docview/2311741904?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals
23. Teixeira da Silva JA, Tsigaris P. Freedom of Information Requests and Peer Review Reports. Science Editor. 2023 Nov 17;
24. Gariépy-Saper K, Decarie N. Privacy of electronic health records: a review of the literature. Journal of the Canadian Health Libraries Association / Journal de l'Association des bibliothèques de la santé du Canada. 2021 Apr 2;42(1).
25. Duan R, Boland MR, Liu Z, Liu Y, Chang HH, Xu H, et al. Learning from electronic health records across multiple sites: A communication-efficient and privacy-preserving distributed algorithm. Journal of the American Medical Informatics Association. 2019 Dec 9;27(3):376–85.
26. Zhang Z, Yan C, Mesa DA, Sun J, Malin BA. Ensuring electronic medical record simulation through better training, modeling, and evaluation. Journal of the American Medical Informatics Association [Internet]. 2020 Jan 1 [cited 2020 Dec 30];27(1):99–108. Available from: https://academic.oup.com/jamia/article/27/1/99/5583723?login=true
27. Tardif D. Understanding privacy risks when accessing electronic medical records. Canadian Journal of Anesthesia/Journal canadien d'anesthésie. 2019 Dec 2;67(2):163–8.
28. Government of Canada IAP on RE. Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2022) – Chapter 2: Scope and Approach [Internet]. ethics.gc.ca. 2023. Available from: https://ethics.gc.ca/eng/tcps2-eptc2_2022_chapter2-chapitre2.html
29. The Personal Health Information Protection Act and Your Privacy [Internet]. Available from: https://www.ipc.on.ca/sites/default/files/legacy/2004/10/phipa-your-privacy-web-e.pdf
30. Scassa T, Kim D. AI Medical Scribes: Addressing Privacy and AI Risks with an Emergent Solution to Primary Care Challenges [Internet]. Ssrn.com. 2025. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5086289
31. McGraw D, Mandl KD. Privacy protections to encourage use of health-relevant digital data in a learning health system. NPJ Digital Medicine [Internet]. 2021 Jan 4;4(1):1–11. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7782585/
32. Privacy and Security Incident Management Protocol [Internet]. 2025 [cited 2025 Mar 26]. Available from: https://www.cihi.ca/sites/default/files/document/privacy-and-security-incident-management-protocol-en.pdf