BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

OPINIONS/PERSPECTIVES/POINT OF VIEW

The Self-Sovereign Patient as a Cornerstone of Healthcare 4.0

Tomer Jordi Chaffer, MSc[1], Joe Littlejohn, MD[2], Arun Nadarasa, MRPharmS[3] and Claudia Lamschtein, MD[4]

[1]Faculty of Law, McGill University, Quebec, Canada; [2]Zucker School of Medicine, New York, New York, USA; [3]International Social Prescribing Pharmacy Association (ISPPA), London, United Kingdom; [4]Department of Psychiatry, Faculty of Medicine, University of Manitoba, Manitoba, Canada

Corresponding Author: Tomer Jordi Chaffer, Email: tomer.chaffer@mail.mcgill.ca

DOI: https://doi.org/10.30953/bhty.v8.414

Keywords: Blockchain, decentralized AI, healthcare 4.0, Self-Sovereign identity

Abstract

In Healthcare 4.0, we are witnessing a fundamental shift from provider-centric systems to patient-centric models, where individuals, empowered by technologies such as blockchain, the Internet of Medical Things, and artificial intelligence (AI), assume the role of the Self-Sovereign Patient, exercising control over their health data and care journey. These technologies enable new forms of data ownership, interoperability, and personalized care, building on the structured reliability of legacy systems. However, significant challenges remain. Tensions between blockchain immutability and regulatory rights such as data erasure, the unresolved question of digital inheritance, and ethical concerns surrounding consent, monetization, and health equity must all be addressed. In addition, institutional barriers such as clinical integration, data governance, and uneven access to digital infrastructure pose risks of deepening existing disparities. AI agents, when responsibly deployed, offer promising pathways to augment care delivery and alleviate workforce burdens. Realizing this vision requires coordinated action across clinical, technical, legal, and ethical domains to design trustworthy, privacy-preserving systems that enhance transparency and accountability.

Plain Language Summary

This article explores how Healthcare 4.0, driven by technologies such as blockchain, artificial intelligence, and Internet of Medical Things, is shifting control of health data from institutions to patients. It explores the concept of the Self-Sovereign Patient, who actively manages and shares their own health information. By using secure, decentralized technologies, patients can give consent, protect their privacy, and participate in new health data ecosystems. The article highlights real-world examples and ethical considerations, showing how these tools can support better care, reduce administrative burden, and increase trust. It also warns that digital access and literacy are essential to ensure these benefits are shared fairly.

Submitted: June 16, 2025; Accepted: August 4, 2025; Published: August 18, 2025

Healthcare is being transformed, not only by new machines but also by a shift in who controls the flow of data, decisions, and trust. Patients are no longer passive recipients of care; they are becoming architects of their own health data ecosystems. The transition to Healthcare 4.0, inspired by Industry 4.0, redefines the patient's role by integrating advanced technologies such as blockchain, artificial intelligence (AI), the Internet of Medical Things (IoMT), and wearables to enhance healthcare delivery, management, and outcomes.[1] Traditionally, medical records, rooted in physician-centric paper charts and later electronic medical records (EMRs), have evolved into electronic health records (EHRs), improving legibility and transferability but maintaining centralized, siloed systems due to inconsistent data standards.[2] Personal Health Records (PHRs) aim to

empower patients by granting data control and requiring consent for access, yet their adoption remains limited, with patient engagement a key challenge.[3] Healthcare 4.0 not only introduces a new technological toolkit but also signals a shift toward decentralized, patient-driven ecosystems that challenge traditional provider-centric models of care.

At the heart of this shift is the Self-Sovereign Patient, an emerging paradigm that positions patients as empowered custodians of their health information, and ultimately as active stakeholders of their health journeys. Here, the Self-Sovereign Patient is one who manages, shares, and benefits from their own health data, acting as a digital custodian within a decentralized healthcare network. To realize this vision, it is essential to view Healthcare 4.0 as a layered architecture: one grounded in legacy systems that manage structured clinical data, and another powered by decentralized, intelligent tools that enable automation, personalization, and patient sovereignty. Indeed, legacy platforms, including EMRs and clinical data warehouses,[4] continue to be the most reliable source of structured, longitudinal data. Despite current limitations such as interoperability challenges, inconsistent data formats, and limited patient access, they serve as the backbone upon which newer technologies will be developed and deployed. To align Healthcare 4.0's promise with the pace of technological innovation, it is crucial to understand the transformative role of technology in shaping healthcare delivery and to anticipate emerging models of care. Preparing clinicians, administrators, bioethicists, and policymakers for these technological shifts is critical to realizing this transformation.

Blockchain technology, when applied to healthcare, offers a distributed and tamper-resistant ledger that ensures data provenance and immutability.[5] A prominent use case of blockchain in healthcare includes Estonia's partnership with Guardtime, which provided a blockchain-based solution to health records of over 1 million citizens.[6] Another notable use case is the MIT Media Lab's MedRec, a decentralized record management system tested within the Harvard Medical School Teaching Hospital's backend systems.[7] Patients, as central administrators of their self-sovereign identities, can manage granular permissions over who accesses their data, when, and for what purpose.[8] This model of transparent, patient-controlled access stands in stark contrast to recent controversies such as National Health Service (NHS) England's Foresight project. In this case, patient data from 57 million general practitioner records, originally collected for COVID-19 research, was used without additional consent to train an AI model, sparking backlash from the British Medical Association and the Royal College of General Practitioners.[9] The lack of transparency and breach of scope highlights why trust-preserving technologies such as blockchain are essential: they offer verifiable access logs and enforceable consent frameworks that could prevent such overreach and restore public confidence in digital health initiatives.

Restoring public confidence in digital health demands scalable, verifiable, and privacy-preserving infrastructure that patients and professionals alike can trust. For instance, Guardtime's advanced blockchain-backed authentication methods such as Keyless Signature Infrastructure (KSI) leverages hash-function cryptography to produce signatures that are cryptographically verifiable, time-stamped, and immune to quantum threats. Because KSI does not require the transmission or storage of raw data but only cryptographic hashes, it guarantees data privacy while enabling scalable, independently verifiable authentication across institutional and geographic boundaries.[10] Building on a foundation of trust, consent mechanisms can be layered with decentralized identifiers (DIDs),[11] verifiable credentials (VCs),[12] or even more recently, soulbound tokens (SBTs),[13,14] which makes it possible for patients to own their data and share only what is necessary with healthcare professionals, insurers, researchers, or even AI agents acting on the behalf of clinicians in the future.[15] Indeed, within Healthcare 4.0, AI agents can act as autonomous or semi-autonomous intermediaries, analyzing real-time health streams and legacy record data to support clinical decisions, triage tasks, or even automate elements of documentation and diagnostics.[16] As Healthcare 4.0 infrastructure continues to be developed and integrated with legacy systems, AI agents could benefit from decentralized AI architectures, such as via secure, distributed evaluation (i.e., assessing models without exposing patient data or proprietary algorithms). In addition, decentralized AI can help reduce bias by drawing on diverse, heterogeneous datasets, which could benefit, for instance, patients with rare diseases.[17] Together, these technologies form the foundation of a secure, patient-directed data ecosystem where AI agents operate not as black boxes but as accountable extensions of clinical care, amplifying human decision-making while preserving patient autonomy and trust.

The IoMT and wearables can continuously generate real-time health data, such as for heart rate variability to sleep cycles and medication adherence.[18] When integrated into a blockchain-based personal health wallet, such as the MediLinker,[19] these data points can inform care plans, trigger smart contracts for automated insurance reimbursement,[20] or alert providers to early warning signs of chronic disease exacerbation.[21] This approach exemplifies the Internet of Medical Technologies (IoMT), where decentralized blockchain infrastructure mitigates single points of failure by securely storing sensor-derived vitals on an immutable ledger, thereby enhancing reliability, traceability, and system resilience.[22] As these systems evolve, the aggregation of IoMT- and wearable-derived data within secure, patient-controlled platforms

Citation: Blockchain in Healthcare Today 2025, **8**: 414 - https://doi.org/10.30953/bhty.v8.414

also lays the groundwork for broader innovation; namely, the development of blockchain-based health data marketplaces. In such models, real-time, high-resolution data streams become valuable digital assets, owned by patients and made available for research, insurance modeling, or AI training under strict consent conditions.[23] If designed with guardrails against the commodification of health data and protections against coercive monetization among vulnerable groups,[24] this paradigm could contribute to a secure and decentralized data-sharing economy that respects consent and incentivizes participation[17] In this way, IoMT-integrated health wallets could not only enhance individual care but also serve as entry points into a broader participatory data economy, one that demands robust governance, ethical safeguards, and institutional readiness to fully realize its transformative potential.

Recent Health Insurance Portability and Accountability Act (HIPAA) directives advocate for secure, patient-centric solutions, emphasizing access to health records, robust cybersecurity, telehealth expansion, and exploring interoperability solutions to address inefficiencies that hinder timely, high-quality care.[25] Like the principle of least-privileged access, HIPAA's minimum necessary standard aims to ensure that access to protected health information is restricted to only what is required for a given task.[24] As blockchain technology continues to expand its use cases within the healthcare space, its application must be carefully aligned with HIPAA's core principles, particularly around access control, data mutability, and encryption. Furthermore, the immutable nature of blockchain also introduces unresolved legal and ethical challenges.[26] Data stored on-chain may be considered permanent, raising tensions with regulatory principles such as the right to erasure or the "right to be forgotten," as established in frameworks like the General Data Protection Regulation (GDPR).[27] In addition, the question of digital inheritance emerges: what happens to a patient's health data after death? As health data gains economic significance, mechanisms must be developed to allow patients to designate trusted heirs, executors, or governance frameworks for posthumous data control and access. Solutions may include social recovery pallets or legally binding digital wills that manage post-mortem data rights.[28] As blockchain becomes more integrated into health ecosystems, privacy-preserving solutions such as zero-knowledge proofs or revocable SBTs will be essential to reconcile permanence with consent, revocation, and inheritance.[29,30] Regulatory frameworks must evolve in tandem with technical innovation, emphasizing ethics by design,[31] explainable and auditable systems, as well as privacy-first solutions.

Yet, these solutions presuppose equal technological access and capability, which is an assumption that does not hold when considering the digital divide. Indeed, realizing this vision must begin with acknowledging the digital divide as a foundational barrier[32] It would not be prudent to assume universal access to smartphones, broadband internet, and IoMT-enabled devices as such infrastructure and affordability remain unevenly distributed across geography, income levels, age, and ability. Without targeted interventions, this disparity risks creating a two-tiered system in which only the digitally resourced can exercise data sovereignty. If left unaddressed, this could undermine autonomy and expose vulnerable populations to exploitation, misinformation, or coercion. Enhancing digital literacy via patient education is essential as sovereignty requires more than technical control but also demands the knowledge, resources, and institutional support that allow patients to exercise that control meaningfully.

Even amid equity challenges, the potential benefits of Healthcare 4.0 technologies remain significant. As these technologies mature, utility applications and intelligent software interfaces—such as mobile dashboards, scheduling assistants, and patient engagement platforms—can streamline clinical workflows and reduce administrative burdens. In a time of global healthcare staffing crises,[33] such tools could act as force multipliers, allowing providers to focus on high-value care activities while AI agents and automated tools manage documentation and coordination tasks. Implementation must contend with challenges such as legacy system compatibility, secure data migration, and staff retraining. Organizational change management will be just as vital as technical integration. Workflow redesigns, cost-benefit analyses, and trust-building will determine whether these tools succeed in amplifying care delivery.

Ultimately, the Self-Sovereign Patient model is a sociotechnical construct that demands institutional change. Clinicians must adapt to patient-generated health data as part of the clinical narrative. Administrators must rethink data governance models. Bioethicists must contend with new questions around autonomy, consent, and equity. Policymakers must anticipate and shape emerging standards that foster trust, transparency, and accountability across digital health ecosystems. The Self-Sovereign Patient model must function not only at the technical layer but also as a trust architecture, thereby enabling policy-aligned data exchange along the stakeholder value chain in ways that reinforce transparency and verifiability. Cross-disciplinary education and scalable systems are vital to support this transformation. And most importantly, we must center the lived experiences of patients in the design of digital health systems. In the end, Healthcare 4.0 is not simply about machines, data, or automation. It is about rehumanizing care by restoring agency to the individual.

Funding

No funding was received.

Conflicts of Interest

The authors have no conflicts of interest to report.

Financial and non-Financial Relationship and Activities

None.

Authors' Contributions

All authors contributed to the conceptualization of the manuscript at various stages of its development. Tomer Jordi Chaffer drafted the initial manuscript and integrated feedback from co-authors. Dr. Joe Littlejohn contributed clinical insights and contextualized the narrative within the broader history of technological transformation in healthcare, including the role of blockchain in Healthcare 4.0. Arun Nadarasa provided analysis of emerging use cases in the participatory data economy and industry applications of blockchain-based solutions. Dr. Claudia Lamschtein contributed ethical analysis, particularly regarding the evolving role of the patient in this new healthcare paradigm. All authors reviewed, revised, and approved the final version of the manuscript for publication.

Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories

This editorial does not contain any primary data analysis or new datasets.

Application of AI-generated Text or Related Technology

We acknowledge the use of ChatGPT (GPT-4o model) to assist with grammar correction, spelling, and editorial refinement throughout the preparation of this manuscript. We also used Claude to support adherence to the Vancouver citation style.

Acknowledgments

Tomer Jordi Chaffer is a member of the Editorial Board for Blockchain in Healthcare Today. We would like to thank Muthu Ramachandran for his helpful suggestions during the preparation of this manuscript.

References

1. Chanchaichujit J, Tan A, Meng F, Eaimkhong S. Healthcare 4.0. Singapore: Springer Nature; 2019.
2. Evans RS. Electronic health records: Then, now, and in the future. Yearb Med Inform. 2016;25(S01):S48–61. https://doi.org/10.15265/IYS-2016-s006
3. Harahap NC, Handayani PW, Hidayanto AN. Functionalities and issues in the implementation of personal health records: systematic review. J Med Internet Res. 2021;23(7):e26236. https://doi.org/10.2196/26236
4. Thantilage RD, Le-Khac N-A, Kechadi M-T. Healthcare data security and privacy in data warehouse architectures. Inform Med Unlocked. 2023;39:101270. https://doi.org/10.1016/j.imu.2023.101270
5. Houtan B, Hafid AS, Makrakis D. A survey on blockchain-based self-sovereign patient identity in healthcare. IEEE Access. 2020;8:90478–94. https://doi.org/10.1109/ACCESS.2020.2994090
6. Heston TF. A case study in blockchain healthcare innovation. Int J Curr Res. 2017;9(11). https://doi.org/10.5281/zenodo.8277804
7. Ekblaw A, Azaria A, Halamka JD, Lippman A. A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. Proc IEEE Open Big Data Conf. 2016;13:13.
8. Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical records. J Am Med Inform Assoc. 2012;20(1):7–15. https://doi.org/10.1136/amiajnl-2012-001023
9. Armstrong S. NHS England faces investigation over granting Foresight access to GP patient data. BMJ. 2025;389:r1192. https://doi.org/10.1136/bmj.r1192
10. Guardtime. KSI Blockchain massive-scale system integrity [Internet]. 2025 [cited 2025 Jun 14]. Available from: https://m.guardtime.com/files/KSI_data_sheet_1805.pdf
11. Kim TM, Ko T, Hwang BW, Paek HG, Lee WY. Self-sovereign management scheme of personal health record with personal data store and decentralized identifier. Comput Struct Biotechnol J. 2025;28:16–28. https://doi.org/10.1016/j.csbj.2024.11.036
12. Mazzocca C, Acar A, Uluagac S, Montanari R, Bellavista P, Conti M. A survey on decentralized identifiers and verifiable credentials. IEEE Commun Surv Tutor. 2025;1–1. https://doi.org/10.1109/comst.2025.3543197
13. Pinna A, Lunesu MI, Tonelli R, Sansoni S. Soulbound token applications: a case study in the health sector. Distrib Ledger Technol Res Pract. 2024;4(3):1–15. https://doi.org/10.1145/3674155
14. Ohlhaver P, Weyl EG, Buterin V. Decentralized society: Finding web3's soul. 2022 [cited 2025 Jun 14]. Available from: https://ssrn.com/abstract=4105763
15. Mukherjee S, Gamble P, Sanz AM, Kant N, Aggarwal K, Manjunath N, et al. Polaris: a safety-focused LLM constellation crchitecture for healthcare[Internet]. arXiv.org; 2024 [cited 2025 Jun 14]. Available from: https://arxiv.org/abs/2403.13313
16. Yuan M, Bao P, Yuan J, Shen Y, Chen Z, Xie Y, et al. Large language models illuminate a progressive pathway to artificial intelligent healthcare assistant. Med Plus. 2024;1(2):100030. https://doi.org/10.1016/j.medp.2024.100030
17. Singh A, Lu C, Gupta G, Behari N, Chopra A, Blanc J, et al. A perspective on decentralizing AI [Internet]. MIT Media Lab; 2025 [cited 2025 Jun 11]. Available from: https://nanda.media.mit.edu/decentralized_AI_perspective.pdf
18. Abdulmalek S, Nasir A, Jabbar WA, Almuhaya MA, Bairagi AK, Khan MAM, et al. IoMT-based healthcare-monitoring system towards improving quality of life: a review. Healthcare. 2022;10(10):1993. https://doi.org/10.3390/healthcare10101993
19. Harrell DT, Usman M, Hanson L, Abdul-Moheeth M, Desai I, Shriram J, et al. Technical design and development of a self-sovereign identity management platform for patient-centric healthcare using blockchain technology. Blockchain Healthc Today. 2022;5(S1):196. https://doi.org/10.30953/bhty.v5.196
20. Mishra AS. Study on blockchain-based healthcare insurance claim system. 2021 Asian Conf Innov Technol (ASIANCON). 2021;1–4. https://doi.org/10.1109/asiancon51346.2021.9544892
21. Bendayan S, Cohen Y, Bendayan J, Windisch S, Afilalo J. Non-fungible tokens in cardiovascular medicine. Can J Cardiol. 2024;40(10):1959–64. https://doi.org/10.1016/j.cjca.2024.07.010

22. Ghadi YY, Mazhar T, Shahzad T, Khan MA, Abd-Alrazaq A, Ahmed A, et al. The role of blockchain to secure internet of medical things. Sci Rep. 2024;14(1):18422. https://doi.org/10.1038/s41598-024-68529-x
23. Chiruvella V, Guddati AK. Ethical issues in patient data ownership. Interact J Med Res. 2021;10(2):e22269. https://doi.org/10.2196/22269
24. Alder S. HIPAA updates and HIPAA changes in 2025 [Internet]. HIPAA J. 2025 [cited 2025 Jun 16]. Available from: https://www.hipaajournal.com/hipaa-updates-hipaa-changes/
25. Hoffman S, Podgurski A. Securing the HIPAA security rule [Internet]. SSRN; 2024 [cited 2025 Jun 16]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=953670
26. Chaffer TJ, Goldston J. On the existential basis of self-sovereign identity and soulbound tokens: an examination of the "self" in the age of Web3. J Strateg Innov Sustain [Internet]. 2022 [cited 2025 Jun 14];17(3). Available from: https://articlegateway.com/index.php/JSIS/article/view/5637/5349
27. Bayle A, Koscina M, Manset D, Perez-Kempner O. When blockchain meets the right to be forgotten: technology versus law in the healthcare industry. In 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), Santiago, Chile. 2018, p. 788–92. https://doi.org/10.1109/wi.2018.00133
28. Goldston J, Chaffer TJ, Osowska J, Charles G. Digital inheritance in Web3: a case study of soulbound tokens and the social recovery pallet within the Polkadot and Kusama ecosystems [Internet]. ArXiv [Preprint]. 2023 [cited 2025 Jun 14]. Available from: https://arxiv.org/abs/2301.11074
29. Bai T, Hu Y, He J, Fan H, An Z. Health-zkIDM: a healthcare identity system based on Fabric blockchain and zero-knowledge proof. Sensors. 2022;22(20):7716. https://doi.org/10.3390/s22207716
30. Boi B, Cirillo F, Santis MD, Esposito C. Soulbound tokens: Enabler for privacy-aware and decentralized authentication mechanism in medical data storage. Blockchain Healthc Today. 2024;7(2):334. https://doi.org/10.30953/bhty.v7.334
31. Ramachandran M. Blockchain engineering: Secure, sustainable frameworks for healthcare applications [Internet]. Singapore: Springer Nature; 2025 [cited 2025 Jun 14]. Available from: https://link.springer.com/book/9789819643592
32. Saeed SA, Masters RM. Disparities in health care and the digital divide. Curr Psychiatry Rep. 2021;23(9):61. https://doi.org/10.1007/s11920-021-01274-4
33. Aluttis C, Bishaw T, Frank MW. The workforce for health in a globalized context – global shortages and international migration. Glob Health Action. 2014;7(1):23611. https://doi.org/10.3402/gha.v7.23611