Internet Medical Journal
ISSN 1093-7935 · medjournal.com · Est. 1996

Specifying Blockchain Audit Infrastructure for Physician-Facing Electronic Health Record Governance

Author(s)	Thomas F. Heston
Affiliation	Department of Family Medicine, University of Washington, Seattle, USA
Affiliation	Department of Medical Education and Clinical Sciences, Elson S. Floyd College of Medicine, Washington State University, Spokane, USA
ORCID	0000-0002-5655-2512

Published	31 May 2026
DOI	10.5281/zenodo.20480516
Article type	Commentary
Citation	Heston TF. Specifying Blockchain Audit Infrastructure for Physician-Facing Electronic Health Record Governance. Internet Medical Journal. 2026;1:e20480516

Abstract

Electronic health records enforce rules about who may open a patient's chart, but they cannot demonstrate that those rules were honored. A recent survey of physicians using a national record system found wide use alongside limited confidence in its privacy protections, and the stated concern was not the absence of access controls but the inability to verify that access was monitored and that its log had not been altered. Blockchain audit infrastructure, a tamper-evident record of access that no single party can change unilaterally, is increasingly proposed as the remedy. Proposing it is not the same as specifying it. Three decisions govern whether such a record earns clinical trust: what it stores, who maintains it, and who controls its rules. This commentary ties each decision to the trust deficit physicians report and argues that any blockchain proposal for clinical records should be required to resolve all three before it is taken seriously.

Keywords

blockchain audit infrastructure, electronic health records, physician trust, patient privacy, access logging, clinical informatics governance, accountability

Electronic health record (EHR) systems typically implement access control mechanisms to restrict which users may open or modify a patient's chart, and they often record these events in audit logs. However, observational and survey data show that clinicians may share accounts, document under another user's identity, or fail to properly log out, practices that undermine strict enforcement and complicate efforts to prove that permissions were consistently honored or that all access was appropriately monitored [1]. This is the gap a recent study of physician attitudes identifies, and it is not closed by tightening the rules governing access [2]. It is closed only by making the access record verifiable and tamper-resistant. Blockchain-based audit logging can provide an immutable, tamper-resistant record of EHR access events, improving the verifiability of access histories, but its contribution to clinical confidence still depends on successful integration, governance, and real-world validation.

The problem is empirical, not hypothetical. A survey of 309 physicians using a national EHR reported that roughly 87% used the system, while only about 56% judged its data protection adequate [2]. The dissatisfaction was precise. The system already governed who could access records; what it could not provide was after-the-fact assurance that access controls had been enforced, that activity had been overseen, or that the access log itself was immune to quiet revision. A control that cannot be shown to have operated provides no real accountability. What is missing is not a stricter policy but a trustworthy account of what the system actually did [3].

A blockchain audit log answers this, and the underlying logic is sound. A blockchain is a shared ledger replicated across several independent parties, so that no one party can alter an entry without the discrepancy becoming evident to the others. Applied to access governance, it records each instance of a record being opened in a form that cannot be rewritten after the fact. This design has been endorsed, with the sound stipulation that no clinical data reside in the ledger, only the record of access events [2]. The endorsement, however, stops short of the decisions that determine whether the design works. A blockchain audit log warrants trust only once three questions about it are answered.

The first question concerns what the ledger stores. The chart, the notes, and patient identity remain in the existing record system and never enter the ledger. The ledger holds only a cryptographic hash of each access event, an irreversible numeric summary that confirms an event occurred without exposing its contents, together with the role, the stated reason, and the identity of the credentialed user. Because the ledger stores one-way hashes rather than clinical text, patient information is neither exposed nor reconstructable from the ledger; privacy is fully preserved.

The second question concerns who maintains the ledger. If the software vendor is the only party holding the ledger, it carries the same opacity that physicians already distrust, because a single party can alter records without being seen. The ledger must therefore be

held simultaneously by several parties whose interests do not align, such as the institution, its privacy office, and an independent auditor. Any attempt by one party to change a record conflicts with the copies held by the others, making the alteration detectable.

The third question concerns who governs the ledger's rules. The automated procedures that write to it, often termed smart contracts, should not be alterable by one party or without notice; amendments should require agreement among the independent parties and a published waiting period, so that a change to the rules is itself part of the auditable record.

None of these provisions is novel, which is the point. The principle of leaving the medical record in place while anchoring a tamper-evident summary of activity to a shared ledger was advanced for clinical research nearly a decade ago in the *Blockchain-based Scientific Study* [4]. The broader argument that physicians should regard blockchain as an instrument of verifiable recordkeeping rather than a financial novelty was made in the same period [5]. The approach was later extended to the provenance of artificial-intelligence-generated text entering the chart, so that the origin and basis of machine-written content remain auditable [6]. What this commentary contributes is the explicit correspondence between those established principles and the measured trust deficit physicians report: the three questions are what separate a defensible concept from a system clinicians would rely on.

To address the technical feasibility, interoperability, and cost challenges of integrating blockchain with existing EHR infrastructures, recent reviews emphasize incremental and hybrid architectures that layer blockchain components alongside legacy systems rather than replacing those systems outright [7]. This measured approach is critical because poorly integrated access control mechanisms can severely disrupt clinical routines. For instance, cumbersome access procedures often force clinicians to develop workarounds due to time constraints, such as postponing documentation, performing work under another user's name, or communicating critical patient information orally rather than recording it, all of which directly compromise patient safety [8]. By operating at the foundational infrastructure layer—similar to how deterministic, privately hosted clinical AI models are managed—blockchain logging can provide an independent, tamper-resistant audit trail without impeding daily clinical tasks. Furthermore, to make this integration feasible across diverse legacy systems, standardizing the underlying audit log data elements and code sets is necessary to ensure that accountability measures are transparent, reproducible, and seamlessly integrated into the provider's workflow.

The corresponding step is small. Any proposal to place clinical access records on a blockchain audit log should state what the ledger stores, who holds the copies that constrain unilateral changes, and who governs its rules. Editors and reviewers assessing such proposals can require these three answers as a standing condition. Until they do, physicians will continue to be offered assurances they cannot independently verify, and the distance between using the record and trusting it will remain where this survey located it.

Declarations

Funding: This study did not receive any external funding.

Conflicts of Interest: The author reports no conflicts of interest.

Data Availability: Not applicable.

Research Ethics Statement: Not applicable. This commentary did not involve human subjects research, animal research, or protected health information.

AI Usage: Large language models were used for language editing and formatting assistance; the author reviewed, verified, and is fully responsible for all content.

References

1. Faxvaag A, Johansen TS, Heimly V, Melby L, Grimsmo A. Healthcare professionals' experiences with EHR-system access control mechanisms. Stud Health Technol Inform. 2011;169: 601–605.

2. Unal C, Yildirim H. A study on physicians' perceptions of privacy in the context of the e-Nabiz (e-Pulse) in the Turkish healthcare system. Sci Rep. 2026 [cited 31 May 2026]. doi:10.1038/s41598-026-53539-8

3. Kannampallil T, Adler-Milstein J. Using electronic health record audit log data for research: insights from early efforts. J Am Med Inform Assoc. 2023;30: 167–171. doi:10.1093/jamia/ocac173

4. Heston TF. The blockchain-based scientific study. Digit Med. 2017;3: 66. doi:10.4103/digm.digm_17_17

5. Heston T. Why Blockchain Technology Is Important for Healthcare Professionals. In: SSRN [Internet]. 20 July 2017 [cited 23 Nov 2017]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3006389

6. Heston TF. Accountable Clinical AI Requires More Than Accuracy. Internet Med J. 2026;1: e19519377–e19519377. doi:10.5281/zenodo.19519377

7. Schmeelk S, Kanabar M, Peterson K, Pathak J. Electronic health records and blockchain interoperability requirements: a scoping review. JAMIA Open. 2022;5: ooac068. doi:10.1093/jamiaopen/ooac068

8. Boonstra A, Jonker TL, Van Offenbeek MAG, Vos JFJ. Persisting workarounds in Electronic Health Record System use: types, risks and benefits. BMC Med Inform Decis Mak. 2021;21: 183. doi:10.1186/s12911-021-01548-0