BLOCKCHAIN® IN HEALTHCARE TODAY
PLATFORM APPROACHES IN HEALTHCARE

OPINIONS/PERSPECTIVES/POINT OF VIEW

Immutability Is Not Trust: Recourse, Reversibility, and the Patient at the End of the Chain

Nuno Galante Valério, MsC in Pharmaceutical Science
Head of Innovation, R&D Quality, Merck Healthcare KGaA, Darmstadt, Germany

DOI: https://doi.org/10.30953/bhty.v9.518

Corresponding Author: Nuno Galante Valério, Email: nf.valerio@gmail.com

Keywords: accountability, immutability, patient safety, recourse, reversibility

Abstract

Blockchain promises records that can never be changed. In healthcare, this is often sold as a way to make data trustworthy. Here, the author argues that an unchangeable record solves only one part of the problem. It proves nobody altered the record after it was written. It does not prove the record was correct, identify who is responsible for it, or allow a patient to challenge a decision that turns out to be wrong. Using data-integrity rules already standard in regulated medicine, the author asserts that correcting mistakes and seeking a remedy are essential to the trust that blockchain in healthcare is meant to deliver.

- An unchangeable record proves only that data were not altered later, not that data were correct to begin with.
- Trustworthy medical systems must let errors be corrected while keeping a permanent, attributed trail of each correction.
- Europe's right to erasure and the European Union Artificial Intelligence (EU AI) Act both assume records can change and decisions can be contested.
- A permanent record of a wrong decision that nobody can appeal protects the record, but it does not protect the patient.
- Regulated medicine solved this decades ago: append the correction, attribute it, timestamp it, and leave the original visible.

Submitted: June 28, 2026, Accepted: July 21, 2026, Published: August 31, 2026

Immutability does one thing, and it does it completely. It guarantees that no one cheats the record. Once a value is written and the block is sealed, no administrator, vendor, or state actor can quietly reach back and change what was said. For a field that grew up and became resilient through data-integrity scandals, falsified trial data, backdated approvals, and the long catalog of reasons the US Food and Drug Administration's electronic records rule, 21 CFR Part 11, exists at all,[1] that is not a minor guarantee.

The trouble starts when the floor gets sold as the building.

Much of the enthusiasm I read in this field treats immutability as though it were trust itself, rather than the first and easiest of trust's requirements. I understand the appeal. When you have spent a career watching records get altered, a record that cannot be altered feels like the answer to everything. But the question a system in medicine actually has to survive is not only "Did someone tamper with this?" But mostly "What happens when this is wrong?" Those are different questions, and the architecture that ensures the first one beautifully is, by nature and construction, at war with the second.

I work on a framework I call Trust Architecture, seven structural functions that every trustworthy system performs before it earns the right to become invisible, drawn comparatively across pharmaceutical regulation, aviation, banking, and nuclear safety. The seven are provenance, verifiability, accountability, reversibility, legibility, recourse, and surveillance. They cluster: provenance and verifiability are the is-it-what-it-claims pair; accountability and reversibility ask whether the thing can be answered for and undone; legibility and recourse ask whether the human affected by it can see what happened and obtain a remedy. Surveillance stands alone, the population-level function that catches the slow harm that no single patient would notice in themselves.

Immutability serves the first pair and is close to nothing else. It makes provenance tamper-evident and verification cheap. That is its whole gift, genuine and real.

But notice what it stays silent on. It tells you the value was not altered after it was written. It tells you nothing about whether the value was right when it was written. Garbage in is garbage in, now preserved forever and harder to challenge precisely because the ledger lends it the authority of permanence. A wrong number that no one can change is not more trustworthy than a wrong number someone can correct. It is actually less.

And on the functions that matter most, when something has already gone wrong (and being healthcare, a human science, that will inevitably happen), immutability is not merely silent. It is hostile. Its entire value proposition is that the past cannot be undone, which is the exact opposite of what reversibility and recourse require.

Here is what the people selling immutability into healthcare tend to miss because many have not lived inside the thing they want to improve. The records I keep in a Good Manufacturing Practice (GMP) environment are sometimes wrong. A value is

mistranscribed, a batch result is later invalidated, and a deviation is raised against a record that looked correct on Tuesday and was understood to be an error by Friday. That happens far more often than the vendors imagine. The regulated world has spent decades on this precise problem, and the standard it reached, ALCOA+, the data-integrity principle I work under every day,[2] does not ask for immutability. It asks for records that are attributable, legible, contemporaneous, original, and accurate; and in the plus, complete, consistent, enduring, and available. Complete is the one that matters here. A complete record includes the correction.

The regulated world's answer, in other words, is a record that is correctable and a correction that is permanent. Immutability offers only the second half and calls it the whole deal. The people who designed data-integrity regulation faced the immutability question a long time ago, and chose against it, on purpose, because they understood that a system you cannot correct is not a safe system. It is an efficient way to make a mistake permanent.

In Europe, this stopped being a matter of engineering taste and became a matter of law. Article 17 of the General Data Protection Regulation (GDPR) gives a person the right gives a person the right to have their personal data erased.[3] A ledger that has written that data into sealed, replicated blocks cannot honor that right without breaking the very property that made it a ledger.

This is not a puzzle a clever lawyer dreamed up. It is a structural collision between a regulation, built on the premise that records about people must stay correctable, and an architecture built on the promise that records can never change. The EU AI Act presses harder still, requiring human oversight and a route for an affected person to contest an automated decision.[4] Recourse and reversibility are not soft preferences in this framework: they have statutory names, and immutability clashes with both.

Beneath the law, there is the patient. Recourse is the function whose absence the post-mortem always finds. The Tuskegee study was not a failure of record-keeping; the records were meticulous.[5] It was a failure of recourse; the people harmed had no mechanism to halt what was being done to them. It is no accident that modern Good Clinical Practice was built afterward to require exactly that: informed consent and the right to withdraw.[6] A flawlessly preserved record of a decision the affected person cannot appeal is not a triumph of trust. It is a flawlessly preserved injustice. Immutability without the rest of the architecture does not protect the patient; it protects the record of what was done to the patient, which is a different thing, and on a bad day, actually the opposite thing.

So, I would offer this field a reframe, as someone who wants it to succeed rather than someone throwing stones from the outside.

Trust is not the absence of error. Nothing that touches medicine promises the absence of error. Trust is what survives error, the capacity of a system to be answered for, to be undone, to be contested by the person it falls on. A system engineered to make the past unchangeable has, with real good intentions, engineered away the mechanism by which trust survives being wrong.

Immutability guarantees the floor. It does not get to bypass the rest of the building. The question worth putting to anyone deploying a permanent ledger in medicine is not how to make the record more permanent, because that capability already exists. It is the harder one that immutability cannot answer on its own: what happens to the patient when the permanent record is wrong?

Funding

This work received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Financial and Non-Financial Relationships and Activities

The author is employed by Merck Healthcare KGaA in a role focused on AI governance for regulated R&D quality. The views expressed are the author's own and do not represent the positions of his employer. The author declares no financial interest in any blockchain or distributed-ledger technology, vendor, or platform discussed in this article.

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

Not applicable.

Application of AI-Generated Text or Related Technology

The author used a large language model as an editing aid – for refining prose and pressure-testing arguments. All claims, framework, sources, and conclusions are the author's own. All AI-assisted text was reviewed, edited, and verified by the author, who takes full responsibility for the content of the article.

Contributors

N.G.V.: conceptualization, writing (initial draft and revision in response to reviewer comments), and final approval of the version submitted for publication.

Acknowledgments

The author thanks the readers of his *The Trust Architecture* newsletter, whose engagement with the public discussion on reversibility and recourse helped sharpen this argument.

References

1. U.S. Food and Drug Administration. 21 CFR Part 11 (Title 21, US Code of Federal Regulations, Part 11: Electronic Records; Electronic Signatures), Silver Spring, MD: FDA; 1997.
2. Medicines and Healthcare Products Regulatory Agency. "GXP" data integrity guidance and definitions. London: MHRA; 2018.
3. European Parliament and Council of the European Union. Regulation (EU) 2016/679 (General Data Protection Regulation), Article 17 (Right to erasure). Off J Eur Union. 2016;L119:1–88.
4. European Parliament and Council of the European Union. Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 14. Off J Eur Union. 2024;L1689:1–144.
5. Brandt AM. Racism and research: the case of the Tuskegee syphilis study. Hastings Cent Rep. 1978;8(6):21–9. https://doi.org/10.2307/3561468
6. International Council for Harmonisation. ICH E6(R3) guideline for good clinical practice. Geneva: ICH; 2025.