

RECORD INTEGRITY

Tamper-evident clinical records: a hash-chain specification for AI-authored documentation

ABSTRACT

United States rules require an electronic health record to have audit controls. They do not require cryptographic tamper-evidence. This paper specifies the construction ChartVoyant uses instead: an append-only event log in which every entry carries a digest over its own content and over the digest of its predecessor, verified by recomputing the chain. It states the threat model the construction covers, separates integrity from provenance, and sets out what a verified chain does not prove.

Type Original technical specification **References** 23 **Reading time** 14 min

Last reviewed September 2026

1 The question a record has to answer once a machine writes in it

When every chart entry was typed by a person, record integrity was mostly a signature problem. Ambient drafting changes the question. When a model produces the first version of a note and a clinician signs the last one, the record must answer three things instead of one: what did the system produce, what did the clinician see, and what did the clinician change.

None of the three survives a history that can be rewritten. If the drafting event can be edited afterward, the difference between a note a clinician composed and one accepted without reading is not recoverable. Integrity is the precondition for any claim about authorship.

ChartVoyant is a voice-first ambulatory EMR. Drafts are produced alongside a transcript that fills live during the visit, and the draft waits: “Nothing signs itself.” Every action, including the model’s, is written to a log that can be added to but not edited or deleted, and each entry is locked to the one before it. The public demonstration makes the failure visible: alter an entry, and “Record verified — every action, including the AI’s” becomes “Record broken at entry 4 — change detected.”

Sections 2 and 3 say why the construction is needed; section 6 says what it does not prove.

2 What the rules actually require, and how little that is

The most-cited audit obligation in United States health IT is one sentence. 45 C.F.R. § 164.312(b), Audit controls, requires a covered entity to “implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.” Nothing sits beneath it: no content list, no retention period, no review cadence.¹

The mechanism that would detect alteration is § 164.312(c)(2), “implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.” It is **addressable**, the weakest tier in the rule, which a covered entity may decline on documented grounds.¹ Section 164.308(a)(1)(ii)(D) is required, but asks only that records of system activity be reviewed “regularly.”² Content requirements come from certification: a module certified to § 170.315(d)(2) must record actions in accordance with § 170.210(e), whose content is fixed by incorporating ASTM E2147-18, and § 170.315(d)(3) requires a sortable audit report.^{3,4} Those criteria bind developers whose modules hold that certification, cited as the source of a requirement, not as a claim about any product.

The useful comparison is 21 C.F.R. Part 11, effective 1997. Section 11.10(e) requires “secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.” Section 11.50 requires a signed record to carry the signer’s name, the date and time, and “the meaning (such as review, approval, responsibility, or authorship) associated with the signature.”⁵ Part 11 reaches only records maintained under FDA requirements, not ordinary EHR use. Still, the regime governing a trial log demands computer-generated tamper-evidence and a stated meaning of signature; the regime governing the chart demands neither.

The January 2025 proposal to overhaul the Security Rule would remove the required/addressable distinction and add a standard at § 164.312(d)(1), “Audit Trail and System Log Controls.”⁶ As of September 2026 it is a proposal, not law. A vendor claiming cryptographic integrity is exceeding what is required of it.

3 Why an ordinary audit log is not enough

An EHR audit log records “who accesses which patient records at what time, and what they do in the record.”⁷ Its evidentiary weight is weaker than its reputation. A systematic review of 85 studies using audit logs to study clinical activity found that only 19 — 22% — validated their results at all, and only 9 — 11% — validated by direct observation, with largely unreported variation in which actions were filtered and how they were mapped to constructs.⁸ Log semantics are vendor-specific and largely undocumented, and there is no standard for what constitutes an “action.”⁹ A log is strong evidence of what a system recorded, not of what happened.

The problem sharpens when a record is contested. Expert witnesses are needed for “recreating an accurate timeline,” because printed renderings of an EHR differ in formatting and chronology from the underlying record;¹⁰ the same authors have published guidance on mitigating audit-log risk in liability cases.¹¹ An analysis of 248 malpractice cases involving health IT found more than 80% with moderate or severe harm, though those were fewer than 1% of the claims in the database.¹²

No amount of log content fixes the problem underneath. An audit log in a mutable database is exactly as trustworthy as whoever administers that database. Log and chart normally share a schema, a backup, a restore path and an administrator. A person with write access can change a row in the chart and the row in the log describing that change, and a reader sees a consistent history.

WHAT THE RECORD-TAMPERING LITERATURE WILL AND WILL NOT SUPPORT

The peer-reviewed forensic literature on record alteration and audit-trail spoliation is thin, and most material surfacing on these topics is expert-witness and law-firm marketing, some carrying unsourced quantitative claims. The malpractice analysis above shows that health-IT-implicated cases tend to involve serious harm, not that EHRs drive a wave of litigation. The case for tamper-evidence rests on what a mutable store makes possible, not on a measured incidence.

4 The specification

Append-only, not immutable

The log admits one operation: append. Entries are never edited and never deleted; a correction, a retraction and an amendment are each new entries referring to an earlier one. Marketing shorthand elides that, including “a record that can’t be changed.” A clinical record cannot be immutable, since patients have amendment rights and clinicians correct what they wrote. It can be append-only, so that nothing is silently overwritten.

Entries and digests

An entry consists of a type drawn from a closed vocabulary, a body, an author, a time, the digest of the entry before it, and its own digest. ChartVoyant’s published vocabulary for a visit is

`visit.transcript.appended` , `ai.note.drafted` , `note.signed` , `claim.submitted` and

`payment.posted`, each carrying its own digest and a pointer to the previous entry's. The first has no predecessor.

“Digest” means a cryptographic digest: a function mapping content of any length to a fixed-length value for which a second input producing the same value cannot feasibly be found. This paper deliberately does not name a function: the choice is a deployment parameter with a finite service life, and what a reader is owed is the construction plus the operator's dated statement of which is in use. Two further requirements are fatal to omit. The bytes fed to the digest must be a canonical serialization, or two honest parties will compute different digests from the same entry. And the digest must cover content, not an identifier: a chain over row identifiers protects nothing inside them.

FIGURE 1

The chain structure. Each digest covers the entry's canonical body together with the digest of the entry before it, so the value at entry k depends on every entry through k .

```

entry 1  visit.transcript.appended
         prev      (none – first entry)
         digest    d1 = H( body1 )

entry 2  ai.note.drafted
         prev      d1
         digest    d2 = H( body2 || d1 )

entry 3  note.signed
         prev      d2
         digest    d3 = H( body3 || d2 )

...

entry k  payment.posted
         prev      d(k-1)
         digest    dk = H( bodyk || d(k-1) )

H        a cryptographic digest function
body_k   canonical serialization of entry k
||        concatenation, in a fixed order

```

Verification and failure

Verification is a walk. Begin at the first entry, which must declare no predecessor. For each entry in order, recompute its digest from the canonical body and the recorded predecessor digest, compare it with the digest recorded on the entry, then confirm that the next entry's recorded predecessor digest

equals the value just computed. The walk needs no privileged access and no secret, which is what makes a public demonstration possible. Chronological linking through cryptographic hashes, so that back- or forward-dating becomes infeasible, was specified by Haber and Stornetta in 1991.¹³ The contribution here is not cryptographic; it is which clinical events become entries.

Alter the body of entry k and its recomputed digest no longer matches the one recorded on it, and every link after k fails the same way. Verification reports the earliest break, which is the position of the alteration, and the remainder is unverifiable until that break is characterized. One damaged entry, from a storage fault as easily as an attack, therefore puts everything after it in question.

TABLE 1

The event vocabulary, what each entry binds, and the consequence of a break at that position.

Event	Author of record	What it binds	What a break here would mean
<code>visit.transcript.appended</code>	Capture path, during the visit	Transcript content as appended	The material the draft came from is unestablished
<code>ai.note.drafted</code>	The model	The draft and its link to the transcript	Machine-drafted text becomes indistinguishable from clinician-composed text
<code>note.signed</code>	The signing clinician	Signed content, signer, time of signing	The attestation loses its subject: which text was affirmed is unknown
<code>claim.submitted</code>	Billing path (837P to clearinghouse)	The claim as submitted	Billing cannot be tied to the documentation supporting it
<code>payment.posted</code>	Remittance path	The posted payment	The financial history cannot be reconciled with the clinical one

Isolation

ChartVoyant states that every practice's data is walled off from every other one, records, files and audit logs alike. Applied here, that yields one chain per practice rather than one global chain: verification and export stay scoped to a single covered entity, and ordering is established within a practice, not between two.

5 Integrity and provenance are different properties

A verified chain proves a history has not changed since it was written. It says nothing about where any assertion in that history came from. A system can hold an excellent chain over a record whose provenance is useless: every entry intact, and no way to tell which reflects a measurement, a copied value, or an inference.

Three bodies of work answer the provenance question differently. The W3C PROV family models provenance around three core types — Entity, Activity, Agent — supporting “identifying an object, attributing the object to person or entity, and representing processing steps.” Of its twelve documents only four are Recommendations; PROV-DM, not the overview, is the normative data model.¹⁴

HL7 FHIR answers with a resource. Provenance carries a `target`, the resources created or modified, and an `agent`, the responsible actors with roles and delegation. It is Maturity Level 4, Trial Use, not normative. And responsibility is divided: Provenance covers the *generation* of an entity, while AuditEvent covers *usage* and all other activity in PROV terms, so a design that records authorship in Provenance and expects it to answer access questions has a gap.¹⁵ That resource is the R5 version, while United States exchange still runs on FHIR R4 (4.0.1, 2018), the base for US Core and certification.¹⁶

Regulation answers a third way, and narrowly. The HTI-1 final rule replaced the legacy clinical decision support criterion with the Decision Support Interventions criterion at 45 C.F.R. § 170.315(b)(11), operative for the CEHRT definition from 1 January 2025.¹⁷ A module must surface source attributes: 13 for evidence-based interventions and 31 for Predictive DSIs, under nine categories running from purpose and input features to external validation, performance and revalidation.^{3,18} It is the closest thing in United States law to a provenance mandate for machine-produced output, and its scope limit is decisive: it attaches to decision support interventions, not to AI-generated documentation. No verified source establishes any United States requirement that a model-drafted note be labeled as machine-authored, and the gap may widen: a December 2025 proposed rule would “fully remove the artificial intelligence (AI) ‘model card’ requirements” from the criterion, though no final rule had issued as of September 2026.¹⁹

6 What tamper-evidence does not prove

A verified chain does not prove the content was true when written: a clinician who documents an examination that did not occur produces an entry that will verify forever. The `note.signed` entry establishes that a signature event occurred, by whom and when, and binds the signed content, but comprehension is not a property any cryptographic construction carries. A chain verifies a wrong note as cleanly as a right one.

The more important limit is structural. A hash chain is evidence against alteration only for a party who can obtain a digest they trust from outside the range under suspicion. An adversary controlling the system, the store and the code that computes digests can alter entry k and recompute every digest from k forward, producing a chain that verifies perfectly. Tamper-evidence then reduces to whether a trusted copy of an expected digest exists beyond that adversary’s reach.

The standard remedy is external anchoring, by trusted timestamping. RFC 3161 defines a Time Stamping Authority that cryptographically binds a hash of the data to a trusted time value, producing evidence “that a datum existed before a particular time.” The authority never examines the underlying

data beyond validating the hash length, so no patient information reaches the service and no business associate question arises.²⁰ ChartVoyant's published description of its audit trail does not claim an external anchor, and this paper does not assert one.

THREAT MODEL

Covered. Alteration or deletion of an entry after the fact by any party with write access to the store, including an administrator, where a verifier can obtain a trusted digest from outside the altered range. Silent overwrite, since the current state is an accumulation rather than a mutable row. Reordering, since each digest depends on its predecessor.

Not covered. An entry that was false when written. Whether a signer read what they signed. The clinical correctness of a draft. An adversary who controls the write path and every copy of an expected digest. Compromise of the software that computes digests at write time, which places the attack before the property begins. *Tamper-evidence* is detection, not prevention. ChartVoyant's security page states that no system is perfectly secure, and nothing here is a guarantee.

7 The blockchain question, answered directly

State the case for a distributed ledger fairly. It supplies two things this construction lacks: external anchoring, since ordering and content commitments are replicated to parties who do not share an administrator with the practice, and the removal of a single administrator as a point of trust.

Then weigh it. The most recent systematic review of blockchain in electronic health records screened 2,692 records and included 16 empirical studies. Thirteen of the 16 — 81% — were prototypes, simulations or architecture designs; three were pilots or case studies; not one was a production-level deployment. Reported throughput ranged from 9 to 210 transactions per second. The review does report a pooled estimate for reduced unauthorized access, but its authors note that the underlying evidence comes from penetration testing, attack simulation and vulnerability modelling rather than real-world breach incidence, so it is not evidence that ledgers reduce breaches.²¹

For a single-practice clinical record, the consensus layer solves a trust problem the setting does not have: one practice is the system of record for its own chart, and no second party's disagreement about ordering needs resolving. What remains once consensus is removed — hash linking and the ordering

guarantee — has been available without it since 1991.¹³ What a ledger buys here is mainly anchoring, which trusted timestamping delivers at lower cost and without disclosing clinical content.²⁰

8 Attribution when a machine is one of the authors

Existing attribution policy absorbs machine drafting without modification, and that is the problem. The Medicare Program Integrity Manual requires the person responsible for a beneficiary's care to be identifiable as such. On scribes it is explicit — “When a scribe is used by a provider in documenting medical record entries (e.g., progress notes), CMS does not require the scribe to sign/date the documentation” — because the treating clinician's signature affirms that the note adequately documents the care provided.²² The whole attestation burden sits with the signing clinician, and nothing requires disclosure of who or what produced the text. Contrast 21 C.F.R. § 11.50, which in FDA-regulated contexts requires a signature to state its meaning, expressly including authorship.⁵

Signing a note a model drafted is therefore a complete legal act and an incomplete record. The signature is the clinician's and so is the responsibility, which the product design supports: suggestions are drafts for a licensed clinician to review, and the AI never decides anything on its own. What the signature does not carry is any trace of the machine's contribution. How liability for ambient AI documentation distributes among clinicians, health systems and vendors is an open question.²³

This is why the drafting event must survive independently of the signed note. If the only durable artifact is the signed note, “what did the clinician change” is answered from whatever versioning the application kept. A specification that takes the question seriously requires three things of the drafting event: that it exist as an entry in its own right, bound into the chain where it occurred; that what it binds be the draft's content, so comparison with the signed text is possible; and that it mark the output as machine-produced, since no regulation compels that labeling. Section 4 provides the first; the others are requirements of the design, not measurements of it.

9 Questions with checkable answers

Tamper-evidence is claimed more often than it is specified. Every claim about an unchangeable record reduces to a few facts that can be checked.

1. Can you verify the record without the vendor, and is anything a verifier needs secret?
2. What does each digest cover: the entry's content, or an identifier for it? And on a break, does the system report the earliest failure's position?
3. Is there an external anchor, and who holds it? If not, the system is defended against a dishonest user, not against whoever controls the platform.

4. Is the AI draft a first-class entry or a field on the signed note, and is its content bound or only the fact of drafting?
5. Is the log isolated per practice, and does that cover verification and export?
6. What does the vendor claim about the truth of the content? The correct answer is nothing: a vendor conflating “unaltered” with “accurate” has not understood its own construction.

The property is narrow, old, cheap to implement and easy to check. When a model writes into a chart, the record of what it produced and what the clinician did with it is the only durable account of how a decision was reached. That account has to be one that nobody, including the vendor, can quietly revise.

REFERENCES

Entries 1 to 6, 14 to 20 and 22 are regulations, standards and agency documents: cite them for the text of a requirement, not as evidence that anything works. Entries 6 and 19 are proposed rules that had not been finalized as of September 2026; neither is law. Entries 7 to 13, 21 and 23 are research and scholarly commentary. Entries 11 and 23 were bibliographically verified but their full texts were not available to this paper, so they are cited for existence and scope only and no specific finding or doctrinal argument is attributed to either.

1. U.S. Department of Health and Human Services, Office for Civil Rights. *Technical safeguards*. 45 C.F.R. § 164.312. [ecfr.gov](https://www.ecfr.gov) **REGULATION**
2. U.S. Department of Health and Human Services, Office for Civil Rights. *Security management process*. 45 C.F.R. § 164.308(a)(1). [ecfr.gov](https://www.ecfr.gov) **REGULATION**
3. Assistant Secretary for Technology Policy / Office of the National Coordinator for Health Information Technology. *2015 Edition health IT certification criteria*. 45 C.F.R. § 170.315. [ecfr.gov](https://www.ecfr.gov) **REGULATION**
4. Assistant Secretary for Technology Policy / Office of the National Coordinator for Health Information Technology, incorporating ASTM International. *Record actions related to electronic health information, audit log status, and encryption of end-user devices*. 45 C.F.R. § 170.210(e), incorporating by reference ASTM E2147-18, *Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems*. [ecfr.gov](https://www.ecfr.gov) **REGULATION**
5. U.S. Food and Drug Administration. *Electronic Records; Electronic Signatures*. 21 C.F.R. Part 11; effective 20 March 1997. [ecfr.gov](https://www.ecfr.gov) **REGULATION**
6. U.S. Department of Health and Human Services, Office for Civil Rights. *HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information*. Notice of proposed rulemaking. 90 Fed. Reg. 898 (Jan. 6, 2025); RIN 0945-AA22; comments closed 7 March 2025. [federalregister.gov](https://www.federalregister.gov) **REGULATION**

7. Sinsky CA, Rule A, Cohen G, et al. *Metrics for assessing physician activity using electronic health record log data*. Journal of the American Medical Informatics Association. 2020;27(4):639–643. [doi:10.1093/jamia/ocz223](https://doi.org/10.1093/jamia/ocz223) MEASURE DEVELOPMENT
8. Rule A, Chiang MF, Hribar MR. *Using electronic health record audit logs to study clinical activity: a systematic review of aims, measures, and methods*. Journal of the American Medical Informatics Association. 2020;27(3):480–490. [doi:10.1093/jamia/ocz196](https://doi.org/10.1093/jamia/ocz196) SYSTEMATIC REVIEW
9. Adler-Milstein J, Adelman JS, Tai-Seale M, et al. *EHR audit logs: A new goldmine for health services research?* Journal of Biomedical Informatics. 2020;101:103343. [doi:10.1016/j.jbi.2019.103343](https://doi.org/10.1016/j.jbi.2019.103343) POSITION PAPER
10. Sittig DF, Wright A. *Identifying a Clinical Informatics or Electronic Health Record Expert Witness for Medical Professional Liability Cases*. Applied Clinical Informatics. 2023;14(2):290. [doi:10.1055/a-2018-9932](https://doi.org/10.1055/a-2018-9932) GUIDANCE
11. Sittig DF, Wright A. *A guide to mitigating audit log-related risk in medical professional liability cases*. Journal of Healthcare Risk Management. 2023;43(2). [doi:10.1002/jhrm.21553](https://doi.org/10.1002/jhrm.21553) GUIDANCE
12. Graber ML, Siegal D, Riah H, et al. *Electronic Health Record–Related Events in Medical Malpractice Claims*. Journal of Patient Safety. 2019;15(2):77–85. [doi:10.1097/PTS.0000000000000240](https://doi.org/10.1097/PTS.0000000000000240) CASE SERIES
13. Haber S, Stornetta WS. *How to time-stamp a digital document*. Journal of Cryptology. 1991;3(2):99–111. [doi:10.1007/BF00196791](https://doi.org/10.1007/BF00196791) PEER-REVIEWED
14. Groth P, Moreau L, eds. *PROV-Overview: An Overview of the PROV Family of Documents*. World Wide Web Consortium, Provenance Working Group. W3C Working Group Note, 30 April 2013. [w3.org](https://www.w3.org) STANDARD
15. Health Level Seven International, Security and Privacy Work Group. *Provenance*. FHIR R5 resource; Maturity Level 4, Trial Use. hl7.org STANDARD
16. Health Level Seven International. *HL7 FHIR Release 4*. Version 4.0.1; published 27 December 2018. hl7.org STANDARD
17. Office of the National Coordinator for Health Information Technology. *Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing*. Final rule. 89 Fed. Reg. 1192–1438 (Jan. 9, 2024); RIN 0955-AA03; effective Feb. 8, 2024. [federalregister.gov](https://www.federalregister.gov) REGULATION
18. Assistant Secretary for Technology Policy / Office of the National Coordinator for Health Information Technology. *9 Key Functionalities and Requirements of the New (b)(11) Decision Support Interventions Certification Criterion*. DSI Explainer series, July 2024. [healthit.gov](https://www.healthit.gov) GOVERNMENT REPORT

19. Assistant Secretary for Technology Policy / Office of the National Coordinator for Health Information Technology. *Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions To Unleash Prosperity*. Proposed rule. 90 Fed. Reg. 60970–61034 (Dec. 29, 2025); RIN 0955-AA09; comments closed Feb. 27, 2026. [federalregister.gov](https://www.federalregister.gov) REGULATION
20. Adams C, Cain P, Pinkas D, et al. *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. IETF RFC 3161, Standards Track. August 2001. rfc-editor.org STANDARD
21. Chandak A, Chandak P, Soni N. *Blockchain applications in electronic health records: a systematic review of qualitative and quantitative evidence*. BMC Medical Informatics and Decision Making. 2026;26:176. [doi:10.1186/s12911-026-03476-3](https://doi.org/10.1186/s12911-026-03476-3) SYSTEMATIC REVIEW
22. Centers for Medicare & Medicaid Services. *Medicare Program Integrity Manual, Chapter 3, § 3.3.2.4 — Signature Requirements*. [cms.gov](https://www.cms.gov) GUIDANCE
23. Gerke S, Simon DA, Roman BR. *Liability Risks of Ambient Clinical Workflows With Artificial Intelligence for Clinicians, Hospitals, and Manufacturers*. JCO Oncology Practice. 2026;22(3):357–361. [doi:10.1200/OP-24-01060](https://doi.org/10.1200/OP-24-01060) POSITION PAPER

RELATED PAPERS

A write-path architecture for an AI-native EMR

What may enter the record, in what state, on whose authority.

Regulating AI in certified EHR technology

What the certification program requires a vendor to disclose about a predictive feature.

Approval gates

The signature event, and what has to be true before it fires.