NEXACC

Audit logging and disclosure accounting policy

NEXACC LLC - HIPAA compliance package v2026.1 - issued 2026-08-31

4750 S 44th Pl Suite 120, Phoenix, AZ 85040 - info@nexacc.com - +1 (443) 739-9197 - www.nexacc.com

What we record, how long we keep it, and how a covered entity can request an accounting of disclosures.

Purpose

This policy implements the audit controls standard at 45 CFR 164.312(b) and supports the accounting of disclosures right at 45 CFR 164.528.

Events recorded

Authentication events: sign-in, sign-out, failed attempts, and password or access changes.

Document events: upload, metadata change, signed-link issuance, and download, each with actor, timestamp, client account, and file reference.

Administrative events: role grants and revocations, client account and membership changes, template and integration changes.

Outbound communications: every email attempt with channel, recipient, subject, delivery status, provider message identifier, and any failure detail.

Data changes: inserts, updates, and status transitions on client records, with the acting identity retained.

Integrity of the log

Audit records are append-only to application roles: the application cannot update or delete entries, and log tables carry policies that deny modification and deletion.

Records are written server-side from the trusted execution path, not from the browser, so a client cannot suppress or forge an entry.

Retention and review

Audit records are retained for at least six years, consistent with the HIPAA documentation retention requirement.

Logs are reviewed on a recurring basis, and immediately following any suspected security incident or unusual access pattern. Findings are documented with the remediation taken.

Accounting of disclosures

A covered entity may request an accounting of disclosures of its PHI by writing to info@nexacc.com.

We respond within 30 days with the date, recipient, description, and purpose of each accountable disclosure within the requested period, up to six years.

Because disclosure activity is derived from retained audit records rather than recollection, the accounting can be produced as an exported record.

Incident and breach handling

Suspected incidents are triaged the same business day, contained, and documented in an incident register with scope, root cause, and remediation.

Where a Breach of Unsecured PHI is confirmed, the covered entity is notified without unreasonable delay and no later than 30 calendar days after discovery, with the information required by 45 CFR 164.410(c).

Questions about this document: info@nexacc.com. NEXACC is not a covered entity; it acts as a business associate to the practices it serves.