healthOS

SECURITY POLICY

Audit Logging

What HealthOS logs, the properties every audit log has, and where each component of an audit record is found.

Edition November 2026 · Public edition · Security: security@healthos.net.au

Contents

What is logged 2

Properties that hold for all of them 3

The key components, and where each is found 3

The NDIA asks for two things: a sample access and event audit log, and a data dictionary that maps the log's attributes to the key components of an audit record. This document is the dictionary. The sample is produced from a non-production stack holding invented data, never from a customer's.

What is logged

LOG	RECORDS	WRITTEN BY
`platform.audit_log`	Every change to a record: who, what, the old and new values	Route handlers and services, on create, update and delete
`audit_access_log`	Every **read** of a clinical record, including refused ones	`middleware/audit-access.ts`, for every route that serves clinical data
`platform.security_events`	Refused cross-tenant and token-misuse attempts	`services/security/security-events.ts` — see security-events.md
`platform.credential_access_log`	Each use of a stored government credential (load, sign, decrypt, refresh)	The integration clients
`platform.integration_auth_failure_log`	Each failed authentication to a government service	The integration clients
Per-integration logs (`integrations.acws_audit_log`, `eclipse_audit_log`, `hi_service_audit_log`, `mhr_audit_log`)	Each call to that government service: operation, outcome, correlation id	The integration clients
Application logs (Log Analytics)	Each HTTP request with its request id, and application events	Pino through Fastify

Properties that hold for all of them

- **Append-only.** Each audit table has a `BEFORE UPDATE OR DELETE` trigger that raises an exception. A row cannot be changed or removed through the application's database role.
- **Retention.** Seven years for the audit tables. Log Analytics retention is 90 days (`infra/modules/container-apps-env.bicep`).
- **Writing never blocks the work.** An audit write that fails is logged (`audit.write.failed`) and the originating request continues.
- **Secrets and identifiers are kept out.** Pino redacts tokens, keys, passwords, Medicare, IHI and DVA numbers, names, dates of birth and addresses before a line is written (`utils/logging/redaction.ts`). The integration logs store a hash of sensitive request parameters, not the parameters.
- **Time.** Every timestamp is `TIMESTAMPTZ`, stored in UTC, set by the database server.
- **Correlation.** `request_id` ties a row to the application log lines of the same HTTP request; `correlation_id` ties an integration row to the government service's own trace.

The key components, and where each is found

AUDIT COMPONENT	`AUDIT_LOG`	`AUDIT_ACCESS_LOG`	`SECURITY_EVENTS`
Who	`performed_by`, `performed_by_name`	`user_id`, `user_name`	`user_id`, `client_id`
When	`performed_at`	`accessed_at`	`occurred_at`
What action	`action`	`action`, `method`	`event_type`, `http_method`
On what	`entity_type`, `entity_id`, `person_id`	`entity_type`, `entity_id`, `person_id`, `path`	`route`
What changed	`old_values`, `new_values`, `changed_fields`	not applicable (a read)	not applicable
Outcome	the row exists only for a completed change	`response_status`	`status_code`, `reason`
From where	`ip_address`, `user_agent`	`ip_address`, `user_agent`	`ip_address`, `user_agent`
Which tenant	`organization_id`	through the user and the person	`organization_id`, `claimed_org_id`
Trace	`request_id`	—	`request_id`

healthOS

Questions about security

Email **security@healthos.net.au**. To report a vulnerability, see https://healthos.net.au/trust/#disclosure.

© 2026 HealthOS Pty Ltd · ABN 81 697 460 889. This is the public edition. The web edition is at https://healthos.net.au/trust/policy-audit-logging.html.