

Financial Insights

Doc type: technical · **Version:** v0.1 · **Status:** published · **Module slug:** financial-insights
Exported: 2026-05-15 11:12 UTC · **By:** anonymous

Financial Insights – Technical Specification

1. Module Purpose & Scope (Authoritative)

Financial Insights provides practices and groups with operational financial intelligence — a clear, timely view of how money is earned, collected, delayed, and distributed across the practice. Its purpose is to turn raw financial data into actionable insight, surface issues early rather than at month-end, and connect diary behaviour, payments, deposits, and subscriptions to financial outcomes so that owners and managers can make informed decisions.

It governs:

- Aggregation of financial signals from Primoro modules and the PMS into a normalised, insight-ready data layer.
- Production of dashboards, reports, trends, forecasts, and AI-generated insight cards.
- Governed cashing-up and associate statement workflows as auditable, approval-gated processes.

It explicitly does not:

- Execute or settle payments — owned by Integrated Payments.
- Enforce booking or deposit rules — owned by Appointment Manager.
- Act as a ledger of record or replace accounting systems such as Xero.
- Make autonomous financial decisions.

2. Ownership & Responsibilities

2.1 Financial Insights IS Responsible For

- Aggregating financial signals from Integrated Payments, the PMS, Subscriptions, Appointment Manager, and HR & People Manager.
- Consuming HR & People Manager data (attendance, overtime, and leave records) as inputs for labour cost calculations, overtime cost analysis, and revenue-per-staff metrics.
- Analysing revenue, collections, deposits, subscriptions, and provider production.
- Producing dashboards, reports, trends, forecasts, and AI-generated insight cards.
- Driving governed follow-up via tasks and alerts when anomalies or risks are detected.
- Providing cashing-up and associate statement workflows as guided, auditable processes.
- Publishing aggregated financial data outputs (revenue aggregates, collections totals, outstanding balances, subscription metrics) as a first-class event feed for consumption by Performance Dashboards.
- Ensuring all calculations are explainable and fully auditable.

2.2 Financial Insights IS NOT Responsible For

- Executing or settling payments — owned by Integrated Payments.
- Enforcing booking or deposit rules — owned by Appointment Manager.
- Holding funds or acting as a ledger of record — outside Primoro scope (accounting system boundary).
- Replacing accounting systems (e.g. Xero) — outside Primoro scope.
- Making autonomous financial decisions of any kind.
- Displaying consolidated performance metrics in the executive dashboard layer — owned by Performance Dashboards (Financial Insights provides the feed; Performance Dashboards owns the presentation).
- Performing financial modelling, labour cost analysis, or revenue-per-staff calculations independently — Financial Insights consumes HR & People Manager attendance, overtime, and leave records as read-only operational inputs and derives labour cost signals from them; the authoritative workforce cost interpretation and staffing analytics remain with HR & People Manager. Financial Insights MUST NOT duplicate or reimplement cost-layer logic that HR & People Manager owns.

3. Core Objects (Normative)

3.1 Financial Signal (Canonical Artefact)

A Financial Signal is a governed, immutable digital artefact representing a normalised, time-bound data point used for insight generation.

Signal types include:

- Revenue event
- Payment received
- Payment refunded
- Payment voided
- Outstanding balance
- Deposit held / converted / forfeited
- Subscription payment status
- Subscription fulfilment order generated (including fulfilment cost vs treatment price for margin tracking)
- Subscription payment failure and retry cycle event
- Subscription mandate cancellation (on subscription end or lapse)
- Subscription fulfilment paused event
- Cash transaction
- Provider production item
- Lab invoice charge / lab invoice chargeback
- Product Shop order revenue / Product Shop refund
- Supplier spend event
- Pipeline estimated value event (read-only; for forecasting purposes only)
- Finance option selected (from Smart Treatment Proposals)
- Finance application initiated (from Smart Treatment Proposals)

Minimum required fields:

- SignalID
- SignalType (enum above)
- SourceModuleReference (FK to originating module record)
- SiteID
- ProviderID (nullable)
- Amount
- CurrencyCode
- SignalTimestamp
- IngestedAt
- AuditTrail (immutable)

For payment-related signals originating from Integrated Payments, the following additional fields **MUST** be populated where applicable:

- PaymentState (Initiated / Authorised / Captured / Refunded / Voided) — reflects the state of the payment at the point of signal emission.
- OriginalPaymentSignalID (nullable) — references the originating payment signal for refund and void corrections.

Signals are immutable once recorded. No update or delete path exists for a Financial Signal; corrections are represented as new offsetting signals with a reference to the original SignalID.

3.2 Insight Card (Canonical Artefact)

An Insight Card is a read-only analytical output surfaced to authorised staff. It contains:

- Title and category (collections / deposits / provider / forecast)
- Supporting data snapshot (references to underlying Financial Signals)
- Plain-English explanation
- Severity (informational / warning / critical)
- Recommended follow-up action (never an automatic action)

Minimum required fields:

- InsightCardID
- Category
- Severity
- GeneratedAt
- AcknowledgedBy (nullable)
- AcknowledgedAt (nullable)
- LinkedTaskID (nullable)
- AuditTrail (immutable)

3.3 Cash Reconciliation Record (Canonical Artefact)

A governed record of a daily cashing-up event, containing:

- ReconciliationID
- Date and SiteID
- ExpectedCashTotal
- CountedCashTotal
- Variance
- VarianceNotes (mandatory when Variance \neq 0)
- VerifierUserID
- ApprovalHistory
- AuditTrail (immutable)

3.4 Provider Statement (Canonical Artefact)

A generated, itemised summary of a provider's production and earnings for a period, containing:

- StatementID
- ProviderID
- PeriodStart / PeriodEnd
- LineItems (production, deductions)
- ApprovalHistory
- ExportedAt (nullable)
- DistributedAt (nullable)
- AuditTrail (immutable)

3.5 Insight Card State Machine (Authoritative)

States:

- **Generated** — AI or scheduled process has produced the card; not yet seen by staff.
- **Acknowledged** — An authorised user has confirmed they have reviewed the insight.
- **Action Created** — A follow-up task has been raised in Task Manager (optional).
- **Resolved** — The underlying issue has been addressed and the card closed.
- **Archived** — Retained for audit; no further actions permitted.

Rules:

- An Insight Card **MUST NOT** transition to Resolved without first passing through Acknowledged.
- State transitions are auditable and time-stamped.
- Insight cards cannot resolve themselves without acknowledgement or an auditable outcome recorded by a human actor.

3.6 Cash Reconciliation State Machine (Authoritative)

States:

- **No Cash Recorded** — No cash entry exists for the site/date.

- **Cash Recorded** — A cash total has been entered but not yet verified.
- **Awaiting Verification** — Record submitted for a second-party check.
- **Verified (Balanced)** — Counted total matches expected; record closed.
- **Verified (Variance Logged)** — Variance recorded with mandatory notes; record closed.
- **Escalated** — Variance breaches a configured threshold; escalation task raised in Task Manager.

Rules:

- A Cash Reconciliation Record **MUST NOT** be marked Verified without a VerifierUserID distinct from the entry author. This enforces a two-person integrity control on cash verification.
- Escalation is triggered automatically when variance exceeds the configured practice threshold; the escalation event is auditable.

3.7 Associate Statement State Machine (Authoritative)

States:

- **Draft Generated** — System has produced the statement from aggregated signals.
- **Under Review** — Statement is open for provider or manager review.
- **Approved** — Authorised approver has sign-off; no further edits permitted.
- **Exported to Accounting** — Statement package dispatched to the accounting integration.
- **Distributed** — Statement delivered to the associate.

Rules:

- Provider Statements **MUST** be in Approved state before export or distribution.
- Once Approved, the statement body is immutable; only distribution metadata may update.

4. Financial Intelligence Capabilities

4.1 Signal Aggregation (Authoritative)

The module **MUST**:

- Ingest Financial Signals from Integrated Payments, PMS, Subscriptions Manager, Appointment Manager, HR & People Manager, Lab Manager, Product Shop, Inventory & Compliance Manager, Care Plan Subscriptions, Hygiene Subscriptions, Smart Treatment Proposals, and Treatment Pipeline Manager on a continuous or scheduled basis.
- Normalise signals into the canonical Financial Signal schema before any analysis or display.
- Process end-of-day and end-of-month scheduled aggregations idempotently so that re-runs produce no duplicate records.
- Ingest payment state-change signals from Integrated Payments covering the full payment lifecycle (Initiated, Authorised, Captured, Refunded, Voided), mapping each state to the appropriate Financial Signal type for reconciliation and revenue attribution.
- Ingest care plan and hygiene subscription billing signals — including monthly recurring revenue events, payment failures and retry cycles, renewal pricing changes, proration events, and suspension events — from Care Plan Subscriptions and Hygiene Subscriptions respectively, so that subscription MRR, churn impact, and payment failure patterns are surfaced in dashboards and Insight Cards.

- Ingest Lab Invoice charge and chargeback signals from Lab Manager for inclusion in provider earnings statements and practice cost analysis.
- Ingest Product Shop order revenue and refund signals for inclusion in cash reconciliation and financial summaries.
- Ingest supplier spend and price variance events from Inventory & Compliance Manager as operational cost signals for practice profitability analysis.
- Ingest pipeline estimated value events from Treatment Pipeline Manager as read-only, forward-looking signals used exclusively for forecasting views; these signals **MUST NOT** be treated as committed revenue.
- Ingest finance option selection and finance application initiation events from Smart Treatment Proposals as informational signals for financial intelligence and insight card generation; these signals do not represent executed transactions.

The module **MAY**:

- Accept manual correction signals initiated by an authorised user (logged as a correcting signal referencing the original).

The module **MUST NOT**:

- Write back to source modules; Financial Insights is a read-and-analyse layer only.
- Modify records in Integrated Payments, Appointment Manager, or any other source module.
- Treat pipeline estimated value signals or finance option selection signals as confirmed revenue or committed transactions.

4.2 Dashboards & Reporting (Authoritative)

The module **MUST** provide:

- Headline metric cards: revenue, collected, outstanding, deposits, subscriptions.
- Trend lines configurable at daily / weekly / monthly granularity.
- Filters by date range, site, provider, and payment method.
- Drill-down from any summary metric to the underlying Financial Signals.
- Group / multi-site views with side-by-side site comparisons and a consolidated vs per-site toggle.
- Drill-through preserved when switching between consolidated and per-site views.

4.3 Insight Card Generation (Authoritative)

The module **MUST**:

- Generate Insight Cards automatically when anomalies, risks, or notable trends are detected.
- Assign each card a severity (informational / warning / critical).
- Include a recommended follow-up that a human must choose to act on; no automatic action is taken.

The module **MAY**:

- Surface AI-generated explanatory text on an Insight Card (subject to AI Boundaries in §7).

The module **MUST NOT**:

- Execute any remediation action autonomously.

- Suppress or auto-resolve an Insight Card without a human acknowledgement.

4.4 Cashing-Up Workflow (Authoritative)

The module MUST:

- Present a daily cash summary card for each site on days when cash is expected.
- Provide a reconciliation screen accepting expected vs counted totals.
- Require mandatory variance notes when counted \neq expected.
- Gate the Verified state behind a second authorised user (two-person integrity).
- Escalate automatically to Task Manager when variance breaches the configured practice threshold.

4.5 Provider Earnings & Associate Statements (Authoritative)

The module MUST:

- Generate draft Provider Statements from aggregated Financial Signals.
- Support RBAC-gated approve and adjust actions.
- Gate export and distribution behind Approved state.
- Provide PDF export and distribution controls.

The module MAY:

- Offer a read-only personal earnings summary view to providers where enabled by practice configuration.

4.6 Performance Dashboards Feed (Authoritative)

Financial Insights MUST produce and maintain an outbound aggregated feed — including revenue aggregates, collections totals, outstanding balances, and subscription metrics — for consumption by Performance Dashboards. This feed is a first-class integration contract; the schema and update cadence are governed jointly by the Financial Insights and Performance Dashboards module owners. Any breaking change to the feed schema MUST be coordinated across both module owners before deployment.

The feed is intended to supply headline aggregates only. Performance Dashboards renders these values as display metrics; it does not perform further financial calculations on them. Financial Insights is the single authoritative source for all financial aggregate values presented in Performance Dashboards.

The feed payload MUST include a `DataFreshnessTimestamp` field on every emitted record, reflecting the timestamp at which the underlying Financial Signals contributing to each aggregate were last processed. Performance Dashboards MUST use this timestamp to render data-currency labels to staff, in accordance with its UX freshness-labelling requirement. The feed is strictly outbound and read-only from the perspective of Financial Insights; Performance Dashboards MUST NOT mutate or write back any financial data.

Financial Insights MUST emit an operational alert if the outbound feed delivery falls outside the agreed update cadence (real-time event stream or micro-batch, to be confirmed in the integration contract per Open Question 5). Feed schema versioning follows the rules in §13.5.

4.7 Subscription Revenue Streams (Authoritative)

Financial Insights MUST aggregate subscription revenue signals from both Care Plan Subscriptions and Hygiene Subscriptions into a unified subscription revenue view. This view MUST surface:

- Monthly recurring revenue (MRR) by subscription programme type.

- Payment failure rates and active retry cycles.
- Churn impact (mandate cancellations and lapsed subscriptions resulting in lost MRR).
- Renewal and proration events contributing to period revenue.

Subscription revenue signals are ingested as Financial Signals per §3.1 and §4.1 and are subject to the same immutability, correction, and audit rules as all other signal types.

5. Delivery Surfaces & Access (Authoritative)

5.1 Web Portal

The primary delivery surface. The Financial Insights Dashboard, Cashing-Up Interface, Provider Earnings screen, and Group / Multi-Site views are all web portal features. All RBAC-gated approval and adjustment actions are performed exclusively through the web portal.

Financial Insights is a distinct navigation destination within the web portal and is not embedded inside the Smart Dashboards landing view. Where the Smart Dashboards module is active, role-appropriate Financial Insights headline metrics (e.g. today's revenue, outstanding balance) MAY be surfaced as a widget or KPI tile within the Smart Dashboards manager view, provided those values are sourced exclusively from the Financial Insights aggregated feed and are rendered read-only. Full Financial Insights functionality — drill-down, cashing-up, provider statements, and insight card management — remains accessible only through the dedicated Financial Insights navigation destination.

5.2 Tablet App

(no content captured in original — needs definition)

5.3 Patient Mobile App

Not applicable. Financial Insights exposes no surfaces in the patient mobile app.

5.4 Engagement Signals

- Insight cards with warning or critical severity surface as notification prompts to authorised staff in the web portal.
- Escalated cash reconciliations generate tasks visible in Task Manager.
- All engagement signals are logged as Audit events so that staff notification history is traceable.

6. Integration Contracts

6.1 Inbound (this module consumes from)

From module	What	Contract
Integrated Payments	Payment lifecycle events (Initiated, Authorised, Captured, Refunded, Voided); outstanding balance updates	Event feed / scheduled sync

PMS	Revenue events, provider production items, cash transactions	Scheduled sync
Subscriptions Manager	Subscription payment status, fulfilment orders, failure/retry events, mandate cancellations, fulfilment paused events	Event feed
Appointment Manager	Booking and deposit events relevant to financial signals	Event feed
HR & People Manager	Attendance records, overtime records, leave records (consumed as read-only inputs for labour cost signals; cost interpretation remains with HR & People Manager)	Scheduled sync
Lab Manager	Lab invoice charge and chargeback events for provider earnings and practice cost signals	Event feed / scheduled sync
Product Shop	Order revenue events and refund events for cash reconciliation and financial summaries	Event feed
Inventory & Compliance Manager	Supplier spend events and price variance metrics for practice profitability analysis	Scheduled sync
Care Plan Subscriptions	Billing signals: MRR events, payment failures, retry cycles, renewal pricing, proration events, suspension events	Event feed
Hygiene Subscriptions	Billing signals: MRR events, payment failures, retry cycles, churn events	Event feed
Smart Treatment Proposals	Finance option selection events and finance application initiation events (informational signals only; no executed transactions)	Event feed
Treatment Pipeline Manager	Pipeline estimated value events (read-only, forecasting use only; not treated as committed revenue)	Event feed / scheduled sync

6.2 Outbound (this module emits to)

To module	What	Contract
Performance Dashboards	Aggregated revenue, collections, outstanding balances, subscription metrics (including <code>DataFreshnessTimestamp</code> per record)	Event feed (first-class integration contract; versioned schema)
Task Manager	Escalation tasks for anomalies, variance breaches, and required approvals	Event / task creation
Communication Hub	Alert notifications to authorised staff for critical insight cards	Event
AI Guardian	Aggregated operational signals (anomalies, deposit irregularities, production outliers); does NOT include raw financial transaction data	Event feed

6.3 PMS Boundary

The PMS is the system of record for clinical appointments, provider production items, and cash transactions. Financial Insights consumes those records via a scheduled sync and normalises them into Financial Signals. Financial Insights **MUST NOT** write back to the PMS. Discrepancies identified in Financial Insights **MUST** be resolved by staff in the PMS or source system; Financial Insights records the observation only.

6.4 External API Gateway & Rate Governance

Any calls Financial Insights makes to external financial data providers — for example, signal enrichment or reporting integrations outside the Primoro platform boundary — **MUST** be routed through the External Provider API Gateway. Such calls **MUST** be classified as BI / background traffic rather than real-time patient-facing traffic, and **MUST** be subject to the rate limits and traffic-isolation rules defined by the gateway for that traffic class. Dashboard refresh cycles that depend on external data sources **MUST** respect the gateway's BI traffic throttling policy. The classification and limits for Financial Insights' external traffic **MUST** be confirmed with the External Provider API Gateway & Rate Governance module owner prior to production deployment.

7. AI Boundaries (Non-Negotiable)

AI MAY:

- Generate plain-English explanations on Insight Cards to help staff understand anomalies.
- Summarise financial trends for human review.
- Flag anomalies and suggest recommended follow-up actions for human consideration.

AI MAY NOT:

- Auto-resolve, auto-acknowledge, or auto-archive Insight Cards.

- Trigger task creation without a human confirmation step.
- Make autonomous financial decisions or commitments on behalf of the practice.
- Bypass RBAC, audit logging, or any governance control.
- Replace required human approval on cash reconciliations or provider statements.

Every AI-generated suggestion displayed on an Insight Card MUST be logged in the audit trail, including whether it was accepted, modified, or dismissed by the reviewing staff member.

8. Audit & Compliance

The system MUST log:

- All Financial Signal ingestion events, including source module reference and ingest timestamp.
- All Insight Card state transitions (Generated → Acknowledged → Action Created → Resolved → Archived), with actor and timestamp.
- All Cash Reconciliation Record state transitions, with actor, timestamp, variance value, and variance notes.
- All Provider Statement state transitions (Draft Generated → Under Review → Approved → Exported → Distributed), with actor and timestamp.
- All user actions: verify, approve, adjust, export, distribute.
- All variance notes entered during cashing-up.
- All exports dispatched to accounting systems, including the destination and export timestamp.
- All AI-generated Insight Card suggestions, including acceptance, modification, or dismissal by the reviewing user.
- All cross-module events consumed (inbound) and emitted (outbound).

Audit logs MUST be immutable and exportable for inspection.

9. Access Control

Access is enforced via Access Manager RBAC. The following capability-to-role mapping is directional; definitive role names and permission levels are owned by Access Manager.

Capability	Who can perform
View dashboards and insight cards	Practice Manager, Owner, authorised staff per RBAC
Acknowledge insight cards	Practice Manager, Owner
Create follow-up tasks from insights	Practice Manager, Owner
Enter cash reconciliation	Designated cashier role
Verify cash reconciliation	Second authorised user (must differ from entry author)
Approve provider statements	Practice Manager, Owner

Adjust provider statements	Practice Manager, Owner (pre-approval only)
Export provider statements	Practice Manager, Owner
Distribute provider statements	Practice Manager, Owner
View personal earnings summary	Provider (where enabled by practice configuration)
Access group / multi-site views	Group Owner, Group Manager

MFA requirements for approval actions (provider statement approval, cash reconciliation verification) are subject to the Access Manager MFA policy; Financial Insights enforces whatever gate Access Manager declares for those sensitive operations.

10. Integration Summary

- **Integrated Payments** — inbound event feed; full payment lifecycle signals (Initiated, Authorised, Captured, Refunded, Voided) and balance signals.
- **PMS** — inbound scheduled sync; revenue, production, and cash transaction signals.
- **Subscriptions Manager** — inbound event feed; subscription lifecycle signals.
- **Appointment Manager** — inbound event feed; booking and deposit financial signals.
- **HR & People Manager** — inbound scheduled sync; labour cost and attendance inputs (read-only; cost interpretation owned by HR & People Manager).
- **Lab Manager** — inbound event feed / scheduled sync; lab invoice charge and chargeback signals.
- **Product Shop** — inbound event feed; order revenue and refund signals.
- **Inventory & Compliance Manager** — inbound scheduled sync; supplier spend and price variance signals.
- **Care Plan Subscriptions** — inbound event feed; billing signals including MRR, failures, renewals, and proration.
- **Hygiene Subscriptions** — inbound event feed; billing signals including MRR, failures, and churn events.
- **Smart Treatment Proposals** — inbound event feed; finance option selection and finance application initiation signals (informational only).
- **Treatment Pipeline Manager** — inbound event feed / scheduled sync; pipeline estimated value signals (forecasting use only).
- **Performance Dashboards** — outbound aggregated financial feed with freshness metadata (first-class integration contract; versioned schema).
- **Task Manager** — outbound task creation for escalations and approval prompts.
- **Communication Hub** — outbound alert notifications for critical insight cards.
- **AI Guardian** — outbound aggregated operational signals (anomalies, outliers); raw transaction data excluded.
- **Access Manager** — RBAC enforcement for all read/write/approve operations.
- **External Provider API Gateway** — rate governance for any external financial data provider calls (BI traffic classification).

11. Explicit Non-Goals

- **Bookkeeping or general ledger** — Financial Insights is insight-only; ledger-of-record functionality belongs to external accounting systems (e.g. Xero).
- **Payment execution or settlement** — owned by Integrated Payments.
- **Booking and deposit rule enforcement** — owned by Appointment Manager.
- **Autonomous financial decision-making** — prohibited; all consequential actions require a human actor.
- **Executive dashboard presentation layer** — owned by Performance Dashboards; Financial Insights supplies the data feed only.
- **Labour cost modelling or staffing analytics** — owned by HR & People Manager; Financial Insights consumes HR outputs as read-only signals only.

12. Versioning & Governance

This specification is owned by: Performance Suite module owner.

Changes to this spec require:

- Review by the Post-MVP module owner.
- Impact analysis across all declared related modules, particularly Performance Dashboards (feed schema changes) and Integrated Payments (signal contract changes).
- Coordination with HR & People Manager owner for any changes to labour cost input contracts.
- Version bump (patch / minor / major) applied per change severity.

13. Build Contract (Engineering & QA)

13.1 Canonical Data Model

(The following represents the governed object shape. Column names and exact table DDL are to be finalised by the engineering team within these field contracts.)

```
financial_signals (  
  signal_id          UUID PRIMARY KEY,  
  signal_type       ENUM(revenue_event, payment_received, payment_refunded,  
                          payment_voided, outstanding_balance,  
                          deposit_held, deposit_converted, deposit_forfeited,  
                          subscription_payment_status, subscription_fulfilment_order,  
                          subscription_payment_failure, subscription_mandate_cancellation,  
                          subscription_fulfilment_paused, cash_transaction,  
                          provider_production_item, lab_invoice_charge,  
                          lab_invoice_chargeback, product_shop_order_revenue,  
                          product_shop_refund, supplier_spend_event,  
                          pipeline_estimated_value, finance_option_selected,  
                          finance_application_initiated),  
  source_module_ref VARCHAR NOT NULL,  
  source_record_id  UUID NOT NULL,  
  site_id           UUID NOT NULL,  
  provider_id       UUID,  
  amount            NUMERIC(14,2) NOT NULL,  
  currency_code     CHAR(3) NOT NULL,  
)
```

```

payment_state          VARCHAR,                -- populated for payment-origin signals
original_payment_signal_id UUID REFERENCES financial_signals(signal_id),
signal_timestamp       TIMESTAMPTZ NOT NULL,
ingested_at           TIMESTAMPTZ NOT NULL DEFAULT NOW(),
is_correction          BOOLEAN NOT NULL DEFAULT FALSE,
corrects_signal_id    UUID REFERENCES financial_signals(signal_id)
)

insight_cards (
  insight_card_id      UUID PRIMARY KEY,
  category             ENUM(collections, deposits, provider, forecast),
  severity             ENUM(informational, warning, critical),
  title               TEXT NOT NULL,
  explanation         TEXT NOT NULL,
  data_snapshot       JSONB,
  recommended_action  TEXT,
  state               ENUM(generated, acknowledged, action_created, resolved, archived),
  generated_at        TIMESTAMPTZ NOT NULL,
  acknowledged_by    UUID REFERENCES users(user_id),
  acknowledged_at    TIMESTAMPTZ,
  linked_task_id     UUID
)

cash_reconciliation_records (
  reconciliation_id    UUID PRIMARY KEY,
  site_id            UUID NOT NULL,
  record_date        DATE NOT NULL,
  expected_cash_total NUMERIC(14,2) NOT NULL,
  counted_cash_total NUMERIC(14,2) NOT NULL,
  variance           NUMERIC(14,2) GENERATED ALWAYS AS (counted_cash_total - expected_cash_total) ST
  variance_notes     TEXT,
  state             ENUM(no_cash_recorded, cash_recorded, awaiting_verification,
                        verified_balanced, verified_variance_logged, escalated),
  entered_by        UUID NOT NULL REFERENCES users(user_id),
  verifier_id       UUID REFERENCES users(user_id),
  verified_at       TIMESTAMPTZ
)

provider_statements (
  statement_id       UUID PRIMARY KEY,
  provider_id        UUID NOT NULL,
  period_start       DATE NOT NULL,
  period_end         DATE NOT NULL,
  line_items         JSONB NOT NULL,
  state             ENUM(draft_generated, under_review, approved, exported, distributed),
  approved_by        UUID REFERENCES users(user_id),
  approved_at       TIMESTAMPTZ,
  exported_at        TIMESTAMPTZ,
  distributed_at     TIMESTAMPTZ
)

```

13.2 Core Behaviour Rules

1. Financial Signals are immutable once recorded; corrections **MUST** be represented as new signals with `is_correction = TRUE` and a valid `corrects_signal_id` reference.
2. An Insight Card **MUST NOT** transition from Generated to Resolved without passing through Acknowledged.

3. Insight cards **MUST NOT** auto-resolve; a human actor with the appropriate RBAC permission **MUST** be recorded on every state transition.
4. A Cash Reconciliation Record with a non-zero variance **MUST** have a non-null `variance_notes` value before it can transition to any Verified state.
5. The `verifier_id` on a Cash Reconciliation Record **MUST** differ from `entered_by`; the system **MUST** reject verification attempts by the same user who entered the record.
6. A Provider Statement **MUST** be in Approved state before it can transition to Exported or Distributed.
7. Once a Provider Statement is in Approved state, its `line_items` payload is immutable.
8. Escalation to Task Manager **MUST** be triggered automatically when a cash reconciliation variance exceeds the configured practice threshold, and the escalation event **MUST** be written to the audit log.
9. The outbound aggregated feed to Performance Dashboards **MUST** update within the cadence defined in the integration contract; failures **MUST** be surfaced as an operational alert.
10. All end-of-day and end-of-month scheduled aggregation jobs **MUST** be idempotent: re-running a job for the same period **MUST** produce no duplicate Financial Signals.
11. All AI-generated insight text **MUST** be logged with the InsightCardID and a record of the human response (accepted / modified / dismissed).
12. Pipeline estimated value signals and finance option selection signals **MUST NOT** be aggregated into committed revenue totals; they **MAY** be used only in forecasting and informational views, clearly labelled as indicative.
13. The outbound Performance Dashboards feed **MUST** include a `DataFreshnessTimestamp` on every record; the feed payload is read-only and **MUST NOT** be mutated by any consuming module.
14. The outbound AI Guardian feed **MUST** contain aggregated operational signals only; raw transaction-level financial data **MUST NOT** be included in signals emitted to AI Guardian.

13.3 Configuration Surfaces

- **Practice-level settings (Admin Control Plane):** cash variance escalation threshold; provider earnings summary visibility toggle (per provider); accounting system export destination; scheduled aggregation windows.
- **Per-user preferences (Access Manager):** notification preferences for critical insight cards.
- **Per-site overrides:** cash reconciliation expected total calculation method (if configurable per site).

13.4 Filtering & Views

The UI **MUST** support the following standard filters on all primary views:

- Date range (preset: today / this week / this month / custom)
- Site (single or multi-select; group-level users see all sites)
- Provider
- Payment method
- Insight severity (for Insight Card list)

Saved filter configurations **MAY** be persisted per user; this is a configurable enhancement and not a hard build requirement for initial delivery.

13.5 Module Extension Map

- Additional Financial Signal types may be added in future without breaking existing signal consumers, provided the `signal_type` enum is extended (non-destructive).
- Additional Insight Card categories may be added without breaking existing card consumers.
- The outbound Performance Dashboards feed schema is versioned; non-breaking additions are minor-version changes; field removal or type changes are major-version changes requiring coordinated deployment.
- The cashing-up and associate statement workflows are designed to be extended with additional approval tiers without restructuring the state machines.

13.6 Acceptance Criteria

The build of Financial Insights is complete when:

- [] All canonical objects (Financial Signal, Insight Card, Cash Reconciliation Record, Provider Statement) can be created and read through the API per the schema in §13.1.
- [] State machine transitions for all four governed objects enforce all rules in §3.5–3.7 and §13.2.
- [] All integrations in §6 are wired and passing contract tests.
- [] AI boundaries in §7 are enforced; negative tests confirm AI cannot auto-resolve cards, auto-create tasks, or bypass RBAC.
- [] Audit log captures every event listed in §8.
- [] Access control is enforced per §9; unauthorised access attempts are rejected and logged.
- [] The cash reconciliation two-person integrity rule (Rule 5) is enforced; self-verification is rejected by the system.
- [] Provider Statement export and distribution are blocked unless state = Approved.
- [] The outbound Performance Dashboards feed is live, schema-validated, and includes `DataFreshnessTimestamp` on every record.
- [] The outbound AI Guardian feed contains aggregated signals only; contract test confirms raw transaction data is absent.
- [] Pipeline estimated value and finance option selection signals are excluded from all committed revenue aggregations; they appear only in clearly labelled forecasting views.
- [] All non-functional requirements in §14 are met.
- [] All scheduled aggregation jobs are verified as idempotent.

14. Non-Functional Requirements

-
- **Performance:** Dashboards MUST update near-real-time as Financial Signals arrive. Dashboard load time for a single-site view MUST remain under a threshold to be defined by the engineering team in the build phase, targeting sub-3-second p95 render for standard date ranges. Scheduled end-of-day aggregation MUST complete within a practice-configurable window (default: overnight).
 - **Reliability:** Scheduled aggregation jobs are idempotent and recoverable; a failed job MUST be retried automatically and MUST NOT produce duplicate signals on retry. Target availability for the Financial Insights dashboard is defined by the Performance Suite SLA, to be established at suite launch.
 - **Scalability:** The module MUST support multi-site, multi-tenant operation; group-level views MUST aggregate across all sites without degrading single-site performance.

- **Security:** All financial data is encrypted at rest and in transit. RBAC is enforced at every read and write boundary via Access Manager; least-privilege access applies. Secrets and credentials for accounting system integrations (e.g. Xero export tokens) MUST be managed through the platform secrets management facility, not stored in application configuration.
- **Privacy:** Financial data containing personally identifiable information (provider earnings, patient payment records) is subject to GDPR rights. Data retention policy for Financial Signals and governed records is to be defined in the platform-wide data retention schedule; Financial Insights MUST honour deletion and export requests routed through the appropriate compliance workflow.
- **Observability:** The module MUST export metrics covering signal ingestion rate, aggregation job success/failure, dashboard load latency, and outbound feed delivery lag. Structured logs MUST be emitted for all state transitions and all cross-module events, with correlation IDs to support distributed tracing across the Performance Suite.

15. Open Questions

1. **Tablet surface scope:** The original specification is silent on whether any Financial Insights capability is exposed on the tablet app. Does the tablet surface any read-only dashboard or insight card view, or is the tablet surface out of scope for this module? (*surfaced from §5.2 gap*)
2. **Cash variance escalation threshold:** What is the default cash variance threshold that triggers escalation to Task Manager, and is it configurable per site or only per practice? (*implied by §4.4 / §3.6 Escalated state — value not defined*)
3. **Provider earnings summary visibility:** The specification states the read-only personal earnings summary is available to providers "where enabled." What is the default state (on or off), and who has permission to toggle it — the practice owner only, or also a manager role? (*implied by §4.5 — not resolved*)
4. **Accounting system export integration:** The specification references export to accounting systems (e.g. Xero) but does not define the integration mechanism, API version, or which accounting systems are in scope for initial delivery. (*referenced in §8 and §13.3 — not resolved*)
5. **Performance Dashboards feed cadence and schema version:** The feed schema and update cadence are described as a first-class integration contract but are not yet specified. What is the agreed update cadence (real-time event stream or micro-batch, to be confirmed in the integration contract) and who owns the schema versioning decision? (*explicitly flagged in §4.6 as needing coordination*)
6. **MFA requirements for sensitive operations:** The specification delegates MFA policy to Access Manager but does not confirm which specific Financial Insights operations (e.g. provider statement approval, cash verification) Access Manager will gate behind MFA. This must be confirmed with the Access Manager module owner. (*implied by §9 — not resolved*)
7. **Smart Dashboards KPI widget scope:** If Financial Insights headline metrics are surfaced as KPI tiles within Smart Dashboards, which specific metrics are included and at what refresh cadence? The exact widget contract must be agreed between the Financial Insights and Smart Dashboards module owners. (*surfaced from §5.1 addition*)
8. **AI Guardian aggregated signal schema:** The outbound feed to AI Guardian is defined as aggregated operational signals (anomalies, outliers). The specific signal types, aggregation window, and schema for this feed must be agreed with the AI Guardian module owner prior to implementation. (*surfaced from §6.2 addition*)