Smart Dashboards

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

Smart Dashboards – Technical Specification

1. Module Purpose & Scope (Authoritative)

Smart Dashboards are the role-based operational awareness layer of Primoro. They surface what matters today and this week, prioritise exceptions, risks, and overdue work, and turn insight directly into action — replacing static reports, exports, and spreadsheet KPIs. Smart Dashboards exist to support day-to-day decision-making, not retrospective analysis.

It governs:

- Role-aware dashboard delivery for all staff types across web and staff app surfaces
- Aggregation and presentation of live signals consumed read-only from source modules
- Direct linking of every dashboard signal to an actionable destination (task, appointment, document, or follow-up)

It explicitly does not:

- Define business logic for any domain — business logic is owned by the source module that produces the data
- Provide historical analytics, performance benchmarking, or target-setting — owned by the Performance Dashboard Suite
- Take autonomous actions without explicit user confirmation

2. Ownership & Responsibilities

2.1 Smart Dashboards IS Responsible For

- Providing and enforcing role-aware dashboards for all staff types (FOH, TCO, Practice Manager/Operator, Practitioner, Dental Nurse)
- Acting as the default landing view after login on both web portal and staff app surfaces
- Aggregating live, read-only signals from across Primoro CORE and any enabled optional modules
- Highlighting overdue, at-risk, and exceptional states using consistent status semantics (On Track / Attention Needed / Overdue / Escalated)
- Linking every dashboard signal directly to the underlying item so that action requires no additional navigation
- Expanding automatically to incorporate widgets from additional Primoro modules as they are enabled
- Enforcing RBAC and site-scoped data governance across all dashboard views, including time-bounded constraints for locum and temporary staff
- Emitting audit events for dashboard access and action launches

2.2 Smart Dashboards IS NOT Responsible For

- Authoring or mutating source data — all writes are owned by the originating module (e.g. Appointment Manager, Task Manager)
- Managing task escalation logic — owned by Task Manager
- Storing or owning ProposalState or conversion data — owned by Smart Treatment Proposals
- Historical trend analysis or BI reporting — owned by Performance Dashboard Suite
- Enforcing access window expiry at the identity level — owned by Access Manager; Smart Dashboards MUST honour the constraints Access Manager enforces
- Data exports as a primary workflow

3. Core Objects (Normative)

3.1 DashboardContext (Canonical Artefact)

A DashboardContext is a governed read-only artefact representing the resolved configuration for a specific user session on a specific site.

Minimum required fields:

- UserId
- Role
- SiteId(s)
- EnabledModules[]

DashboardContext is resolved at session initialisation and re-evaluated on any role, site, or module-enablement change.

3.2 DashboardCard (Canonical Artefact)

A DashboardCard is a governed display unit representing a single metric or signal surfaced on a role dashboard.

Minimum required fields:

- CardId
- RoleScope
- SourceModule
- MetricType
- Status (OnTrack | Attention | Overdue)
- ActionLink (deeplink reference to underlying item)

3.3 AlertSignal (Canonical Artefact)

An AlertSignal is a governed notification of an exception or risk state surfaced from a source module.

Minimum required fields:

- SourceModule
- Severity
- LinkedEntityId

- EscalationState

3.4 Dashboard State Rules (Authoritative)

- Dashboards MUST reflect live source-module state; no stale local copy may be treated as authoritative.
- Every AlertSignal MUST link to an actionable destination; signals without an ActionLink MUST NOT be displayed.
- Optional module widgets MUST appear only when the corresponding module is enabled in EnabledModules[].
- Locum and temporary staff accounts MUST NOT surface admin-surface or manager widgets, regardless of the role assigned.
- Where a locum's access window has expired mid-session, the dashboard MUST redirect to the login screen on the next refresh or interaction.

4. Role-Based Dashboard Surfaces (Authoritative)

4.1 Role-First Design

Dashboards are determined by who is logged in, automatically tailored by role, and zero-configuration by default. Each role sees only what is relevant to their responsibilities.

Common roles include: Front-of-House (FOH), Treatment Coordinator (TCO), Practice Manager / Operator, Practitioner, Dental Nurse.

4.2 Today & This Week Orientation

Dashboards focus on today and the immediate week ahead. Month-end reporting and historical trend analysis are deliberately excluded from CORE dashboards; such views require the Performance Dashboard Suite to be enabled.

4.3 Insight → Action Flow

Every dashboard signal MUST:

- explain why attention is needed
- link directly to the underlying item
- allow action without requiring a report export or additional navigation

Insight without a direct action path is considered an incomplete implementation.

4.4 FOH Dashboard

The module MUST surface:

- Today's appointments with status coding
- Unconfirmed / cancelled / no-show alerts
- Waitlist matches
- FOH task queue
- Inline actions: confirm, arrive, cancel, take payment

4.5 TCO Dashboard

The module MUST surface:

- Treatment pipeline (presented → accepted → declined), consuming data exclusively from Smart Treatment Proposals
- Follow-up dates and overdue actions
- Conversion actions (call, email, schedule)
- TCO task list

The module MAY surface:

- Care plan and finance widgets, when the relevant optional modules are enabled

4.6 Manager / Operator Dashboard

The module MUST surface:

- Live operational KPIs (CORE set only)
- Overdue tasks and escalations
- Compliance and risk alerts
- Cross-team visibility
- Multi-site roll-up, when authorised and enabled

4.7 Practitioner Dashboard

The module MUST surface:

- Personal schedule (today)
- Forms and aftercare status
- Lab and referral awareness
- Practitioner task list
- Quick links to clinical record

4.8 Nurse Dashboard

The module MUST surface:

- Daily clinical checklists
- Assigned surgery context
- Decontamination and compliance tasks
- Lab and referral tracking
- Nurse task list

4.9 Staff App Mode — Mobile Card Contract

Smart Dashboards are the authoritative owner of DashboardCard definitions and AlertSignal logic across all surfaces, including Staff App Mode. Staff App Mode surfaces role-scoped DashboardCards and AlertSignals as defined by this module; it does not define or override card or signal logic.

When DashboardCards are rendered within Staff App Mode, the following mobile-specific contract applies:

- Smart Dashboards MUST provide a mobile-friendly card representation for every DashboardCard it defines; this representation MUST include at minimum the `CardId`, `Status`, a human-readable summary, and a valid `ActionLink` that resolves correctly on a mobile surface.
- AlertSignals surfaced via Staff App Mode MUST conform to the same `AlertSignal` schema defined in §3.3; no separate mobile-only signal schema is permitted.
- RBAC and site-scope enforcement defined in §9 applies equally to DashboardCards and AlertSignals rendered within Staff App Mode. Staff App Mode MUST NOT surface cards or signals outside the user's authorised role and site scope.
- Staff App Mode is responsible for the presentation layer (layout, navigation, and interaction patterns) on mobile. Smart Dashboards is responsible for the content contract (which cards and signals are available for a given role, their status, and their action destinations).

5. Delivery Surfaces & Access (Authoritative)

5.1 Web Portal

Smart Dashboards act as the default landing view after login on the staff web portal. Role-appropriate dashboards are rendered immediately; optional module widgets load asynchronously to avoid blocking the primary view.

5.2 Staff App (Mobile)

Smart Dashboards act as the default home view on the staff app. The staff app surface has a defined primary content contract distinct from the web view.

The staff app dashboard MUST surface as primary signals, in order:

- **Tasks** — the user's open and due task queue
- **Updates** — relevant alerts, notifications, and workflow changes since last login
- **Rota highlights** — the user's scheduled sessions and any coverage gaps relevant to their role

Additional role-specific cards (e.g. appointment lists, forms status) MAY appear below these primary signals where screen space and role scope permit, subject to the same RBAC rules as the web surface.

Staff App Mode consumes DashboardCard and AlertSignal data from Smart Dashboards as defined in §4.9. Smart Dashboards provides the mobile-friendly card representation; Staff App Mode is responsible for rendering and navigation on the mobile surface.

5.3 Patient Mobile App

Smart Dashboards do not surface on the patient mobile app. *(no content captured in original — needs definition if this changes)*

5.4 Engagement Signals

Dashboard access events and action launches are emitted as audit events. Source modules consume no signal back from Smart Dashboards; the data flow is strictly inbound to the dashboard layer.

6. Integration Contracts

6.1 Inbound (this module consumes from)

From Module	What	Contract
Appointment Manager	Schedule state, appointment status	Near real-time read
Task Manager	Open tasks, escalation state	Near real-time read
Communication Hub	Message volume and responsiveness signals	Near real-time read
Digital Forms	Form completion state	Near real-time read
Rota Manager	Coverage context, scheduled sessions	Near real-time read
Smart Treatment Proposals	ProposalState, conversion outcomes (presented → accepted → declined)	Near real-time read
Payments & Pipeline	Pipeline and payment state (when enabled)	Near real-time read
Access Manager	RBAC role, site scope, locum/temporary flags, access window	Session-time enforcement
External PMS (e.g. Dentally)	Schedule and record data, via owned modules	Via source module boundary

Appointment Manager — Governed Read-Only Data Interface

Appointment Manager exposes a governed read-only data interface for external consumers, including Smart Dashboards. Smart Dashboards MUST consume appointment data exclusively through this interface and MUST NOT attempt direct access to Appointment Manager's underlying data store.

The interface provides the following minimum fields per appointment record surfaced to Smart Dashboards:

- `AppointmentId` — unique identifier for the appointment
- `PatientId` — identifier of the linked patient record
- `SiteId` — site at which the appointment is scheduled
- `PractitionerId` — identifier of the assigned practitioner
- `ScheduledAt` — ISO 8601 datetime of the appointment
- `Status` — current appointment status (e.g. Confirmed, Unconfirmed, Arrived, Cancelled, NoShow, Completed)
- `AppointmentType` — type or treatment category descriptor
- `ActionableFlags` — structured flags indicating states requiring attention (e.g. unconfirmed, overdue payment, incomplete form)

Access to this interface is subject to the same RBAC and site-scope rules enforced across all Smart Dashboard integrations; Smart Dashboards MUST NOT request or cache appointment records outside the authenticated user's authorised SiteId(s). Smart Dashboards MUST treat Appointment Manager's interface as the authoritative source for schedule state and MUST NOT treat any dashboard-layer copy of appointment data as authoritative.

6.2 Outbound (this module emits to)

To Module	What	Contract
Audit & Compliance	Dashboard access events, action launch events	Async event
Task Manager	Action launches from dashboard signals (user-initiated)	Deeplink / event

6.3 PMS Boundary

The external PMS (e.g. Dentally) is the system of record for clinical schedule data. Smart Dashboards do not integrate directly with the PMS; they consume PMS-sourced data only as surfaced through owned Primoro modules (primarily Appointment Manager). Smart Dashboards MUST NOT treat dashboard-layer copies of PMS data as authoritative.

7. AI Boundaries (Non-Negotiable)

Module does not embed AI surfaces directly.

The Module Extension Map (§13.5) identifies AI Guardian as a future optional integration that would surface risk-pattern signals as AlertSignals. When AI Guardian is enabled, the following boundaries apply to its signals as presented through Smart Dashboards:

AI MAY:

- Surface risk pattern alerts as AlertSignals for human review
- Summarise exception states to assist staff in prioritising attention

AI MAY NOT:

- Auto-decide on any action surfaced on a dashboard
- Bypass RBAC, site-scope, or audit checks
- Make commitments on behalf of the practice
- Replace required clinical judgement

7.1 AI Assistant (Aiden) — Signal Consumption Boundaries

Aiden (AI Assistant) may surface and contextualise AlertSignals and DashboardCard states originating from Smart Dashboards in order to assist staff in understanding and prioritising their workload. The following boundaries govern this interaction:

- Aiden MAY read and present AlertSignals and DashboardCard status values as produced by Smart Dashboards. Aiden MUST NOT re-evaluate, override, or contradict the signal state as defined by the authoritative source module.

- Aiden MUST NOT surface a Smart Dashboards AlertSignal to a user who would not otherwise have visibility of that signal under RBAC and site-scope rules. Smart Dashboards MUST ensure that any signal made available for Aiden consumption is tagged with the `RoleScope` and `SiteId` constraints that govern its visibility.
- Signals surfaced to Aiden MUST carry a `SourceModule` reference so that Aiden can attribute the signal correctly and direct the user to the appropriate actionable destination via the `ActionLink`.
- Where an AlertSignal carries an `EscalationState` or a DashboardCard carries a `Status` of `Overdue` or `Attention`, these values represent the authoritative assessment of the source module. Aiden MAY summarise or contextualise these states but MUST NOT downgrade or dismiss them.
- Smart Dashboards does not define confidence thresholds for Aiden's language model behaviour; however, AlertSignals made available for Aiden consumption MUST only be signals with a valid `LinkedEntityId` and a resolvable `ActionLink`. Signals that fail either condition MUST NOT be rendered on any surface, including via Aiden.

8. Audit & Compliance

The system MUST log:

- All dashboard access events, including UserId, Role, SiteId, and timestamp
- All action launches from dashboard signals (e.g. task opened, appointment acted on), including the LinkedEntityId and actor
- Role-based visibility enforcement decisions (i.e. when a card or widget is suppressed due to RBAC scope)
- Locum access window expiry events and resulting session redirects

Audit logs for dashboard events are owned by this module and emitted to Audit & Compliance. Smart Dashboards MUST NOT duplicate audit records already owned by source modules. All audit logs MUST be immutable and exportable for inspection in accordance with platform-wide compliance requirements.

9. Access Control

Access is governed via Access Manager using role-based visibility.

Action	Who
View own role dashboard	All authenticated staff
View manager / operator widgets	Practice Manager / Operator role only
View multi-site roll-up	Authorised multi-site users only
Configure role-to-dashboard mapping	Admin (Admin Control Plane)
Configure threshold definitions	Admin (Admin Control Plane)
Configure site visibility	Admin (Admin Control Plane)

Rules:

- No cross-role data leakage is permitted.
- Sensitive metrics MUST be hidden from non-authorised roles.
- Site-scoped data MUST be enforced for multi-site users; users see only sites within their authorised SiteId(s).
- Locum and temporary staff MUST land on the standard role dashboard for their assigned role with no elevated access to manager-surface or admin-surface widgets.
- Admin-surface cards, multi-site roll-up views, and configuration widgets MUST be suppressed for any account flagged as locum or temporary, regardless of role assignment.
- Smart Dashboards MUST NOT cache or persist a locum user's session beyond the access window granted by Access Manager.

MFA requirements for dashboard access are governed by Access Manager policy and are not separately defined at the dashboard layer.

10. Integration Summary

- **Appointment Manager** — inbound near real-time read of schedule and appointment status via Appointment Manager's governed read-only data interface (see §6.1)
- **Task Manager** — inbound near real-time read of task queue and escalation state; outbound deeplink on user action
- **Communication Hub** — inbound near real-time read of message volume and responsiveness signals
- **Digital Forms** — inbound near real-time read of form completion state
- **Rota Manager** — inbound near real-time read of coverage context and scheduled sessions
- **Smart Treatment Proposals** — inbound near real-time read of ProposalState and conversion outcomes (authoritative source for TCO pipeline widgets)
- **Payments & Pipeline** — inbound near real-time read of pipeline and payment state (when enabled)
- **Access Manager** — RBAC, site scope, locum/temporary flags, and access window enforcement
- **Audit & Compliance** — outbound immutable event log for access and action launch events

11. Explicit Non-Goals

- **Historical analytics and BI reporting** — deliberately excluded from CORE; would be owned by Performance Dashboard Suite if added.
- **Deep historical trend analysis** — excluded from CORE; owned by Performance Dashboard Suite.
- **Unrestricted per-user customisation** — dashboards are role-determined and zero-configuration by default; bespoke per-user layouts are out of scope.
- **Altering source data** — Smart Dashboards are strictly read-only; all writes are owned by source modules.
- **Operating without RBAC enforcement** — not permissible under any configuration.
- **Data exports as a primary workflow** — out of scope; export tooling is owned by source modules or Performance Dashboard Suite.

12. Versioning & Governance

This specification is owned by: the Primoro CORE module owner.

Changes to this spec require:

- Review by the MVP module owner
- Impact analysis across all declared related modules (see /propose)
- Version bump (patch for clarifications, minor for capability changes, major for contract-breaking changes)

All future changes MUST preserve:

- Role-first design
- Actionable-signal focus
- CORE vs Performance Dashboard Suite separation
- RBAC governance and audit requirements

13. Build Contract (Engineering & QA)

13.1 Canonical Data Model

```
DashboardContext (
 user_id             UUID NOT NULL,
 role                VARCHAR NOT NULL,
 site_ids            UUID[],
 enabled_modules     VARCHAR[]
)

DashboardCard (
 card_id             UUID PRIMARY KEY,
 role_scope          VARCHAR NOT NULL,
 source_module       VARCHAR NOT NULL,
 metric_type         VARCHAR NOT NULL,
 status              ENUM('OnTrack', 'Attention', 'Overdue') NOT NULL,
 action_link         TEXT NOT NULL
)

AlertSignal (
 alert_id            UUID PRIMARY KEY,
 source_module       VARCHAR NOT NULL,
 severity            VARCHAR NOT NULL,
 linked_entity_id    UUID NOT NULL,
 escalation_state    VARCHAR NOT NULL
)
```

13.2 Core Behaviour Rules

1. Dashboards MUST reflect live source-module state; no stale local copy may be treated as authoritative.
2. No dashboard MAY surface data outside the user's RBAC scope (role and site).
3. Every AlertSignal MUST link to an actionable destination; signals without a valid ActionLink MUST NOT be rendered.
4. Optional module widgets MUST appear only when the corresponding module is listed in EnabledModules[].

5. Performance analytics MUST remain outside CORE dashboards regardless of configuration.

6. Locum and temporary staff accounts MUST NOT surface admin-surface or manager widgets, regardless of role assignment.

7. Where a locum's access window has expired mid-session, the dashboard MUST redirect to the login screen on the next refresh or interaction.

8. TCO pipeline and conversion widgets MUST consume data exclusively from Smart Treatment Proposals.

9. Staff app dashboard MUST surface Tasks, Updates, and Rota highlights as the three primary signals before any additional role-specific cards.

10. Optional widgets MUST load asynchronously and MUST NOT block rendering of the primary dashboard view.

11. Appointment data MUST be consumed exclusively via Appointment Manager's governed read-only data interface; Smart Dashboards MUST NOT treat any dashboard-layer copy of appointment data as authoritative.

12. AlertSignals and DashboardCard states made available for consumption by AI Assistant (Aiden) MUST carry valid `RoleScope`, `SiteId`, `LinkedEntityId`, and `ActionLink` values; signals missing any of these MUST NOT be surfaced on any surface, including via Aiden.

13. Staff App Mode MUST receive a mobile-friendly card representation for every DashboardCard, including at minimum `CardId`, `Status`, a human-readable summary, and a valid mobile-resolvable `ActionLink`.

13.3 Configuration Surfaces

Configuration	Configurable By	Where
Role-to-dashboard mapping	Admin	Admin Control Plane
Threshold definitions (where supported)	Admin	Admin Control Plane
Site visibility for multi-site users	Admin	Admin Control Plane
Optional module enablement	Admin	Admin Control Plane

13.4 Filtering & Views

Dashboards support:

- Role-scoped views only (no cross-role browsing)
- Site switching, where the user holds authorisation for multiple sites
- Today / This Week toggles on time-sensitive widgets

13.5 Module Extension Map

The following optional modules extend Smart Dashboards when enabled, without breaking this contract:

Module	Extension

Performance Dashboard Suite	Trend and analytics views appended to Manager/Operator dashboard
Care Plans	Membership insight widgets on TCO dashboard
Finance	Financing and pipeline state widgets
Inventory	Stock alert signals
AI Guardian	Risk pattern surfacing as AlertSignals

13.6 Acceptance Criteria

The build of Smart Dashboards is complete when:

- [ ] All authenticated users land on the correct role dashboard on login
- [ ] Only data within the user's RBAC scope (role and site) is visible
- [ ] Overdue and at-risk states are highlighted using consistent status semantics
- [ ] Every dashboard signal links to an actionable destination
- [ ] Optional module widgets appear and disappear cleanly based on EnabledModules[]
- [ ] Staff app dashboard surfaces Tasks, Updates, and Rota highlights as primary signals
- [ ] Locum accounts are restricted to role-appropriate dashboard; admin-surface widgets are suppressed
- [ ] TCO pipeline and conversion widgets consume data exclusively from Smart Treatment Proposals
- [ ] Expired locum sessions redirect to login on next refresh or interaction
- [ ] All audit events in §8 are captured and emitted to Audit & Compliance
- [ ] Access control rules in §9 are enforced, including negative tests for cross-role and cross-site leakage
- [ ] Appointment data is consumed exclusively via Appointment Manager's governed read-only interface; dashboard-layer copies are not treated as authoritative
- [ ] AlertSignals and DashboardCards made available for Aiden consumption carry valid RoleScope, SiteId, LinkedEntityId, and ActionLink values
- [ ] Staff App Mode receives a mobile-friendly card representation for every DashboardCard with the required minimum fields
- [ ] All non-functional requirements in §14 are met

14. Non-Functional Requirements

- **Performance:** Dashboard primary view MUST render without waiting for optional widget data. Optional widgets load asynchronously. Core dashboard data SHOULD be served from a cache layer; cache freshness policy is to be defined by engineering to balance latency against data staleness.
- **Reliability:** No dashboard failure MAY block core operational workflows. Dashboard unavailability MUST degrade gracefully, allowing staff to navigate directly to source modules. Availability target to be defined by engineering; the module SHOULD target parity with the platform-wide SLA.
- **Scalability:** Dashboard context resolution MUST support multi-site, multi-tenant configurations. Site switching MUST not expose data from unauthorised sites. Widget loading MUST remain performant as EnabledModules[] grows with additional optional modules.

- **Security:** All data in transit MUST be encrypted. All data at rest MUST be encrypted in accordance with platform-wide key management policy. No cross-role or cross-site data leakage is permitted under any configuration. Time-bounded locum access windows MUST be enforced at the dashboard layer; expired sessions MUST redirect to login.
- **Privacy:** Smart Dashboards surface patient-linked data (e.g. appointment and form status) and MUST honour the platform's GDPR rights obligations. Retention policy for dashboard audit events is to be aligned with the platform-wide audit log retention standard, to be confirmed with the Audit & Compliance module owner.
- **Observability:** Smart Dashboards MUST export: (a) dashboard load latency per role; (b) widget render success/failure rates per SourceModule; (c) RBAC suppression event counts; (d) session redirect counts for expired locum windows. Metrics, logs, and traces MUST be emitted in the platform-standard observability format.

15. Open Questions

1. **Cache freshness policy:** The original notes that dashboards load with "cached core data" but does not define the maximum acceptable staleness window. What is the target cache TTL for core dashboard data, and how is cache invalidation triggered when source-module state changes?
2. **Availability target:** No specific availability SLA is stated for Smart Dashboards. What is the target uptime, and what is the defined graceful degradation behaviour when one or more source modules are unavailable?
3. **Performance latency targets:** No specific load-time targets are defined. What are the P50/P95 dashboard render time targets for web and staff app surfaces?
4. **MFA requirement:** It is not specified whether any dashboard actions or configuration surfaces require MFA. Does access to manager-surface or admin-configuration widgets require MFA step-up, or is session authentication sufficient?
5. **Patient app applicability:** The original is silent on whether any Smart Dashboard surface will ever appear in the patient mobile app. Is this a permanent non-goal or deferred scope?