

Campaign Manager

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

Campaign Manager – Technical Specification

1. Module Purpose & Scope (Authoritative)

Campaign Manager is Primoro's event-driven marketing orchestration and intelligence layer. It enables practices to design, segment, compose, and attribute multi-step marketing campaigns and journeys, using Primoro's mobile app as the primary delivery channel. It solves the problem of fragmented, channel-siloed outreach by providing a single governed engine that connects patient lifecycle events to structured, consent-safe marketing activity.

No campaign triggering, segmentation, enrolment, messaging, optimisation, attribution, reporting, builder behaviour, or AI logic may operate outside the rules defined in this specification.

It governs:

- Definition, persistence, and lifecycle management of Campaigns, Journeys, Campaign Templates, and Builder Schemas
- Dynamic audience segmentation over Primoro's shared canonical data model
- Visual drag-and-drop campaign and journey composition via the Builder Engine
- Event-driven enrolment, pausing, resumption, exit, and suppression logic
- Campaign performance analytics and attribution contracts
- AI-assisted (Aiden) campaign ideation, template selection, optimisation, and insight (advisory only)

It explicitly does not:

- Function as a CRM — no module within this scope owns that concern
- Own message delivery, channel arbitration, throttling, or quiet-hours enforcement — those are owned by Communication Hub
- Manage clinical recalls or emergency communications — those concerns are out of scope for a marketing-only module
- Reclassify, progress, or mutate pipeline state — that is owned by Treatment Pipeline Manager
- Replace advertising platforms — external advertising is out of scope

2. Ownership & Responsibilities

2.1 Campaign Manager IS Responsible For

- Definition and persistence of Campaigns, Journeys, Campaign Templates, and Builder Schemas
- Visual campaign and journey composition via a governed, declarative Builder Engine
- Audience segmentation computed dynamically over shared Primoro data (no duplicated contact stores)
- Event-driven enrolment, pausing, resumption, and exit logic

- Marketing-only cadence, branching, throttling intent, and suppression rules
- Declaring frequency cap and contact fatigue constraints (enforced at execution by Communication Hub)
- Campaign performance analytics and attribution contracts
- AI-assisted (Aiden) campaign ideation, template selection, optimisation, and insight — advisory only
- Immutable audit logging of all campaign lifecycle events (see §8)

2.2 Campaign Manager IS NOT Responsible For

- Message delivery, channel selection, quiet hours, or send-time throttling — owned by Communication Hub
- Storage or maintenance of patient, lead, or contact records — owned by the shared canonical data model; no local copies are permitted
- Clinical recall scheduling — not a marketing function; out of scope
- Emergency communications — owned outside this module; Campaign Manager enforces active exclusion of emergency stacks
- Pipeline state mutations (stage progression, lead reclassification) — owned by Treatment Pipeline Manager
- Revenue visualisation UI — owned by Performance Dashboards; Campaign Manager provides data feeds only
- Concierge interaction state or behaviour — owned by AI Concierge

3. Core Objects (Normative)

3.1 Campaign (Canonical Artefact)

A Campaign is a governed digital artefact representing a discrete marketing construct comprising:

- audience definition (segment, trigger, or event-based)
- one or more Campaign Steps composed via the Builder Engine
- optional entry, exit, and suppression conditions
- measurable objectives (engagement, booking, conversion, revenue)

Campaigns may be one-off, scheduled, or continuously-eligible (dynamic).

Minimum required fields:

- CampaignID
- PracticeID (FK to owning practice)
- CampaignState
- CreatedBy (user/role)
- CreatedAt
- AuditTrail (immutable)

3.2 Campaign State Machine (Authoritative)

States:

- Draft
- Scheduled

- Active
- Paused
- Completed
- Cancelled

Rules:

- All state transitions are auditable and time-stamped.
- A Campaign **MUST NOT** return to Draft once it has reached Active state.
- A Campaign **MAY** be Paused from Active state and resumed back to Active.
- A Campaign transitions immediately to Paused or Cancelled on a suppression event; silent continuation is prohibited under all circumstances.
- Only users with the Approve/Activate permission (see §9) may transition a Campaign from Scheduled or Draft to Active.

3.3 Campaign Step

Each Campaign Step defines:

- channel intent (in-app / email / WhatsApp / SMS)
- content reference(s)
- timing and delay rules
- optional branching and behavioural conditions

No Campaign Step may send directly. All steps execute through Communication Hub.

3.4 Journey

A Journey is an ordered, conditional orchestration of Campaign Steps and/or Campaigns.

Journeys:

- are strictly marketing-only constructs
- may branch based on engagement events or upstream lifecycle changes
- **MUST** immediately relinquish control on suppression events (see §4.2)

3.5 Campaign Builder Engine (Drag-and-Drop)

Campaign Manager **MUST** expose a visual, drag-and-drop campaign and journey builder engine.

The Builder Engine:

- allows users to compose Campaign Steps visually
- supports drag-and-drop ordering and branching
- enforces only marketing-permitted actions (no booking creation, no pipeline mutation)
- validates structure before activation; invalid or unsafe flows **MUST** be rejected
- persists campaigns as structured, declarative schemas — not executable code

Builder output **MUST** be entirely declarative and auditable.

4. Shared Data Layer & Event Architecture (Normative)

Campaign Manager operates on Primoro's shared canonical data model.

- No local copies of patients, leads, or contacts exist within Campaign Manager.
- All segmentation is computed dynamically over shared data.

4.1 Event Subscriptions (Read-Only)

Campaign Manager subscribes to events from:

Source Module	Events / Signals Consumed
Treatment Pipeline Manager	Lead transitions, Opportunity outcomes, Segmentation Events (see §5.1)
Communication Hub	Delivery, open, click, reply signals
Appointment Manager	Marketing-safe booking signals
Loyalty & Rewards	Milestones, anniversaries
Loyalty Insights	Structured handoff signals triggering campaign eligibility (see §4.4)
Smart Treatment Proposals	Proposal creation, acceptance, stalling events (where module enabled)
AI Concierge	Engagement and outcome signals (where AI Concierge module is enabled)
Recall & Reconnect	Patient enrolment events (used as suppression signals — see §4.3)
Care Plan Subscriptions	Enrolment and upgrade campaign eligibility signals (where module enabled — see §4.5)

AI Concierge signals. AI Concierge MAY emit the following outcome signals to Campaign Manager upon completion of a concierge interaction:

Signal	Description
<code>concierge.contact.reached</code>	The concierge successfully made contact with the recipient.
<code>concierge.contact.accepted</code>	The recipient accepted the concierge's offer or proposal (e.g. agreed to book or proceed).

<code>conciierge.contact.declined</code>	The recipient explicitly declined; Campaign Manager MUST treat this as a suppression signal for the associated campaign goal.
<code>conciierge.contact.no_answer</code>	The concierge attempted contact but received no response; may be used as a re-entry or follow-up trigger.

All AI Concierge signals are consumed read-only. Campaign Manager MAY use these signals to:

- inform audience segmentation (e.g. excluding contacts already reached or accepted)
- trigger or suppress subsequent Campaign Steps based on concierge outcome
- annotate engagement telemetry for reporting purposes

Campaign Manager MUST NOT use AI Concierge signals to mutate concierge state or alter concierge behaviour.

4.2 Suppression & Exit Events (Non-Negotiable)

Campaign enrolment MUST immediately stop when:

- a Lead books an appointment
- an Opportunity converts, closes, or is withdrawn
- explicit marketing consent is revoked
- a patient is enrolled in an active Recall & Reconnect journey (see §4.3)
- an AI Concierge recovery workflow emits a suppression lifecycle signal for the contact (see below)
- a Loyalty Insights handoff triggers a competing campaign request that Campaign Manager determines would create a collision with an active campaign (see §4.4)

Silent continuation is prohibited under all circumstances.

AI Concierge recovery-workflow suppression. During AI Concierge recovery workflows, the AI Concierge module MAY emit suppression lifecycle signals beyond the standard outcome signals listed in §4.1. Campaign Manager MUST treat any such signal — specifically signals indicating that the concierge has assumed active responsibility for re-engagement with a given contact — as a suppression trigger for all concurrent marketing campaigns targeting that contact. This prevents campaign collisions during concierge-led recovery. Campaign Manager MUST NOT resume suppressed steps for that contact until a terminal concierge outcome signal (`conciierge.contact.accepted`, `conciierge.contact.declined`) is received, or until a configurable concierge-hold timeout elapses. The timeout value is a practice-level configuration setting.

4.3 Recall & Reconnect Enrolment Suppression

Recall & Reconnect is a deterministic, rules-based module that publishes patient enrolment events to the shared event bus. Campaign Manager MUST subscribe to these enrolment events and apply suppression to any concurrent marketing campaigns targeting the same patient.

The interaction contract is as follows:

- When Recall & Reconnect emits a patient enrolment event, Campaign Manager MUST evaluate all active campaigns in which the patient is currently enrolled and suppress any whose campaign type would conflict with a concurrent recall journey (specifically: nurture, keep-informed, and drip campaign types).

- Suppression triggered by Recall & Reconnect enrolment **MUST** be logged with the reason code `RECALL_RECONNECT_ENROLMENT` and is subject to all standard audit requirements (§8).
- Because Recall & Reconnect is fully deterministic and rules-based (not AI-inferred), Campaign Manager **MUST** treat its enrolment events as authoritative suppression signals without requiring additional validation.
- If both Campaign Manager and Recall & Reconnect are simultaneously active on the same patient, the Recall & Reconnect journey takes precedence; Campaign Manager **MUST NOT** re-enrol the patient into suppressed campaign types until a Recall & Reconnect exit event is received.
- Campaign Manager **MAY** resume suppressed campaigns once Recall & Reconnect emits a journey-completion or patient-exit event, subject to normal suppression and consent re-evaluation at that time.

4.4 Loyalty Insights Handoff Collision Prevention

Loyalty Insights emits structured handoff signals that may indicate a patient's eligibility for campaign or outreach activity. Campaign Manager **MAY** consume these signals as campaign-trigger inputs, but **MUST** evaluate each incoming handoff signal against currently active campaigns before creating or progressing any enrolment.

- If a Loyalty Insights handoff would result in a patient receiving concurrent campaign messages from two independently triggered campaigns, Campaign Manager **MUST** apply its contact fatigue and frequency cap rules (§6.1) to determine which campaign proceeds.
- Handoff-triggered campaigns are subject to all standard suppression and exit rules; a Loyalty Insights handoff signal does not override suppression.
- The resolution of collisions between handoff-triggered campaigns and other active campaigns **MUST** be logged in the audit trail.

4.5 Care Plan Subscriptions Integration

Where the Care Plan Subscriptions module is enabled, Campaign Manager **MAY** receive enrolment nudge and upgrade recommendation signals from that module. These signals indicate that a patient may be eligible for a care plan enrolment or upgrade campaign.

- Care Plan Subscriptions signals are consumed read-only and used solely to populate or update audience segments for care-plan-related campaigns.
- Campaign Manager **MUST** emit suppression or segmentation events to Care Plan Subscriptions (via the shared event bus) to prevent care plan enrolment campaigns from colliding with other active outreach targeting the same patient.
- All care-plan-related campaign activity is subject to standard consent, suppression, and audit rules. No care plan enrolment may be created or progressed by a Campaign Manager campaign; Campaign Manager declares campaign intent only.

5. Integration with Treatment Pipeline Manager

5.1 Pipeline-Initiated Segmentation

Treatment Pipeline Manager emits Segmentation Events when:

- a Lead becomes cold or nurture-eligible
- an Opportunity is Lost, Deferred, or Won with future potential

Campaign Manager **MAY**:

- use these events as segment entry signals only

Campaign Manager MUST NOT:

- reclassify, progress, or alter pipeline state

Segmentation Event contract. The following event names and required payload fields constitute the normative integration contract between Treatment Pipeline Manager and Campaign Manager. Engineering MUST implement this handoff exactly as specified.

Event Name	Emitted When	Required Payload Fields
<code>pipeline.lead.cold</code>	A Lead has received no qualifying activity within the configured cold threshold	<code>lead_id</code> , <code>practice_id</code> , <code>source_channel</code> , <code>cold_since_timestamp</code> , <code>eligible_campaign_types[]</code>
<code>pipeline.lead.nurture_eligible</code>	A Lead is explicitly flagged by Treatment Pipeline Manager as suitable for nurture marketing	<code>lead_id</code> , <code>practice_id</code> , <code>source_channel</code> , <code>nurture_reason</code> , <code>eligible_campaign_types[]</code>
<code>pipeline.opportunity.lost</code>	An Opportunity has been marked Lost	<code>opportunity_id</code> , <code>lead_id</code> , <code>practice_id</code> , <code>source_channel</code> , <code>lost_reason</code> , <code>lost_at_timestamp</code>
<code>pipeline.opportunity.deferred</code>	An Opportunity has been marked Deferred	<code>opportunity_id</code> , <code>lead_id</code> , <code>practice_id</code> , <code>source_channel</code> , <code>deferred_until_date</code> , <code>eligible_campaign_types[]</code>
<code>pipeline.opportunity.won_future_potential</code>	An Opportunity is Won but Treatment Pipeline Manager has flagged further marketing potential	<code>opportunity_id</code> , <code>lead_id</code> , <code>practice_id</code> , <code>source_channel</code> , <code>won_at_timestamp</code> , <code>future_potential_context</code>

The `source_channel` field identifies the originating pipeline stack (e.g. `standard`, `emergency`) and MUST be used by Campaign Manager to enforce emergency exclusion rules (see §5.2). The `eligible_campaign_types[]` array is an advisory hint from Treatment Pipeline Manager; Campaign Manager retains final authority over campaign selection and MUST validate eligibility against its own suppression and consent rules before enrolment.

5.2 Emergency Exclusion

Emergency Stacks (\leq 72-hour pipelines) MUST be excluded from:

- nurture campaigns
- keep-informed journeys
- drip or long-horizon marketing flows

This exclusion is enforced at the campaign engine level and **MUST NOT** be overridden by campaign configuration.

Emergency Stack record lifetime alignment. Treatment Pipeline Manager defines Emergency Stacks as having a maximum record lifetime of 72 hours. Campaign Manager **MUST** align its exclusion logic with this constraint: if a contact's `source_channel` identifies an emergency pipeline and the record has not been resolved within 72 hours, Campaign Manager **MUST** continue to suppress all excluded campaign types until an explicit pipeline resolution event is received (e.g. `pipeline.opportunity.lost`, `pipeline.opportunity.won_future_potential`). Campaign Manager **MUST NOT** assume that the passage of 72 hours alone constitutes resolution; suppression is lifted only upon receipt of a terminal pipeline event for the relevant record.

6. Audience Segmentation (Dynamic & Platform-Native)

Campaign Manager supports dynamic, rule-based segmentation across:

- Leads
- Patients
- Referral Partners

Segments may reference:

- Treatment Pipeline Manager attributes (stage, stack, outcome)
- Appointment history and status (via Appointment Manager)
- Proposal status and age (where Smart Treatment Proposals module is enabled)
- Engagement telemetry (opens, clicks, replies)
- Consent state and channel eligibility

Audience membership is evaluated at send time, ensuring real-time accuracy.

6.1 Frequency Caps & Contact Fatigue Rules (Normative)

Campaigns **MAY** declare contact-level frequency and fatigue constraints, including:

- maximum marketing touches per contact per defined period
- minimum time between marketing touches
- exclusion of contacts currently enrolled in other active campaigns

These constraints are:

- declared by Campaign Manager
- enforced by Communication Hub
- evaluated at execution time

Contact fatigue rules **MUST NOT** be bypassed by campaign configuration.

7. AI Boundaries (Non-Negotiable)

Campaign Manager embeds AI surfaces via Aiden, the platform AI assistant.

AI (Aiden) **MAY**:

- propose new Campaign or Journey drafts (created in Draft state only — never Active)
- suggest Builder layouts (steps, delays, channels)
- recommend pre-defined Campaign Templates
- suggest audiences based on pipeline stalls, proposal inactivity, and engagement patterns
- summarise campaign performance for human review
- surface optimisation recommendations from analytics data
- consume campaign status and suppression state in read-only mode to inform suggestions (e.g. avoiding recommendations for contacts currently suppressed)

AI (Aiden) MUST NOT:

- auto-activate campaigns
- auto-enrol contacts into campaigns
- auto-send messages
- override consent, suppression, or emergency exclusion rules
- make commitments on behalf of the practice
- bypass governance, audit, or access checks
- replace required clinical or compliance judgement
- reference individual-level AI Quality Monitor findings (e.g. documentation gaps or quality issues attributed to named staff members) as suppression triggers, audience-segmentation criteria, or campaign-targeting inputs — doing so would constitute surveillance-by-design and is prohibited; AI Quality Monitor data MUST NOT flow into Campaign Manager's segmentation or suppression logic under any circumstances
- initiate any action that mutates campaign state, enrolment records, or suppression lists; Aiden's relationship to Campaign Manager is strictly read and advisory

All AI output is advisory, explainable, and auditable. All AI-generated Campaign or Journey drafts MUST be reviewed, edited if appropriate, and explicitly activated by a human before any enrolment or delivery occurs.

8. Audit & Compliance

The system MUST log:

- Campaign and Journey creation, edits, and deletion events, with actor and timestamp
- Builder Engine configuration changes
- All Campaign state transitions, with actor and timestamp
- Audience snapshots at campaign execution time
- Enrolment, exit, and suppression events, with explicit reason codes for suppressed sends (including `RECALL_RECONNECT_ENROLMENT` and `CONCIERGE_RECOVERY_HOLD` where applicable)
- Consent enforcement outcomes per Campaign Step
- AI suggestion provenance for every Aiden-generated draft, template, or recommendation, including whether each suggestion was accepted or rejected by a human
- All cross-module events emitted or consumed (see §6.1 Integration Contracts)

All audit logs MUST be immutable, timestamped, and exportable for inspection.

Audit logs **MUST** be retained in accordance with the platform-level data retention policy and must support export on request for regulatory inspection.

9. Access Control

Access control is enforced via Access Manager roles. The following operations require the stated access levels:

- **Create** Campaign, Journey, or Template — requires a role with campaign authoring permission, as defined in Access Manager
- **Read** campaign analytics and performance data — requires a role with campaign read permission
- **Update / Edit** Draft or Paused campaigns — requires campaign authoring permission
- **Activate / Approve** (transition Campaign to Active) — requires a distinct Approve permission; the same user who created a campaign **MUST NOT** be the sole approver unless the practice is configured as a single-operator practice — this constraint requires team confirmation; see §15
- **Pause / Cancel** active campaigns — requires campaign management permission
- **Delete** Draft campaigns — requires campaign authoring permission; Active or Completed campaigns **MUST NOT** be deleted; they may only be Cancelled

MFA requirements for sensitive operations (e.g. bulk campaign activation or consent-rule overrides) are governed by Access Manager and must be confirmed during build — see §15.

10. Delivery Surfaces & Access (Authoritative)

10.1 Web Portal

Campaign Manager is the primary staff-facing surface. The web portal exposes:

- the drag-and-drop Builder Engine for Campaign and Journey composition
- audience segment builder and preview
- campaign status dashboard (draft / scheduled / active / paused / completed)
- analytics and attribution reporting views
- AI (Aiden) suggestion surfaces within the builder

10.2 Tablet App

(no content captured in original — needs definition)

10.3 Patient Mobile App

Patients do not interact with Campaign Manager directly. The Primoro Patient Mobile App is the preferred delivery channel for campaign messages executed by Communication Hub; Campaign Manager declares channel intent, and Communication Hub manages app-channel delivery.

10.4 Engagement Signals

Campaign Manager emits campaign-level engagement telemetry (delivery, open, click, reply, conversion) for consumption by Performance Dashboards. It does not own the visualisation layer.

11. Integration Contracts

11.1 Inbound (this module consumes from)

From Module	What	Contract
Treatment Pipeline Manager	Segmentation Events (<code>pipeline.lead.cold</code> , <code>pipeline.lead.nurture_eligible</code> , <code>pipeline.opportunity.lost</code> , <code>pipeline.opportunity.deferred</code> , <code>pipeline.opportunity.won_future_potential</code>)	Async event
Communication Hub	Delivery, open, click, reply, and unsubscribe/STOP signals	Async event
Appointment Manager	Marketing-safe booking signals (used as suppression triggers)	Async event
Loyalty & Rewards	Milestone and anniversary events	Async event
Loyalty Insights	Structured handoff signals indicating campaign eligibility (used as trigger inputs subject to collision prevention — see §4.4)	Async event (where module enabled)
Smart Treatment Proposals	Proposal creation, acceptance, and stalling events	Async event (where module enabled)
AI Concierge	Concierge outcome signals (<code>concierge.contact.reached</code> , <code>concierge.contact.accepted</code> , <code>concierge.contact.declined</code> , <code>concierge.contact.no_answer</code>) and recovery-workflow suppression lifecycle signals	Async event (where module enabled)
Recall & Reconnect	Patient enrolment events (used as suppression triggers — see §4.3)	Async event (where module enabled)
Care Plan Subscriptions	Enrolment nudge and upgrade recommendation signals (used to populate audience segments — see §4.5)	Async event (where module enabled)

11.2 Outbound (this module emits to)

To Module	What	Contract
-----------	------	----------

Communication Hub	Campaign Step execution requests — content references, channel intent, attribution IDs, metadata	Async event
Performance Dashboards	Campaign performance and attribution data feeds	Async / data feed
Audit & Compliance	Immutable audit events for all campaign lifecycle activity	Async event
Care Plan Subscriptions	Suppression and segmentation events to prevent care plan enrolment campaign collisions (where module enabled — see §4.5)	Async event

11.3 PMS Boundary

Campaign Manager does not integrate directly with the PMS. Patient and appointment data is accessed via Primoro's shared canonical data model; any PMS-sourced data is surfaced through that shared layer, not via a direct Campaign Manager–PMS integration.

12. Integration Summary

- **Communication Hub** — outbound campaign step execution; inbound delivery, engagement, and suppression signals
- **Treatment Pipeline Manager** — inbound segmentation events; Campaign Manager must not mutate pipeline state
- **Appointment Manager** — inbound marketing-safe booking signals used as suppression triggers
- **Loyalty & Rewards** — inbound milestone and anniversary events for campaign triggers
- **Loyalty Insights** — inbound structured handoff signals used as campaign-trigger inputs, subject to collision prevention (§4.4)
- **Smart Treatment Proposals** — inbound proposal lifecycle events (where module enabled)
- **AI Concierge** — inbound concierge outcome and recovery-workflow suppression signals (where module enabled); read-only
- **Recall & Reconnect** — inbound patient enrolment events used as suppression triggers; Campaign Manager yields to active recall journeys (§4.3)
- **Care Plan Subscriptions** — inbound enrolment and upgrade eligibility signals; outbound suppression/segmentation events to prevent campaign collisions (§4.5)
- **Performance Dashboards** — outbound data feeds for campaign analytics and attribution visualisation
- **Access Manager** — RBAC for all create/read/update/activate/delete operations
- **Audit & Compliance** — immutable event log for all campaign lifecycle activity

13. Explicit Non-Goals

- **CRM functionality** — Campaign Manager is not a CRM; no module in this scope owns general CRM capability.
- **Advertising platform replacement** — external paid advertising is out of scope.
- **Clinical recall management** — a dedicated recall module (not yet in scope) would own this if added.
- **Emergency communications** — Campaign Manager actively excludes emergency stacks from all marketing flows; emergency outreach is out of scope.
- **Message delivery and channel arbitration** — owned by Communication Hub; Campaign Manager declares intent only.
- **Revenue visualisation UI** — owned by Performance Dashboards; Campaign Manager provides data feeds only.

14. Non-Functional Requirements

- **Performance:** Campaign state transitions and enrolment/suppression events **MUST** be processed within a latency acceptable for real-time suppression (i.e. a booking or consent-revocation event **MUST** halt enrolment before any subsequent Campaign Step executes). Specific latency targets to be defined at build. (*target thresholds need confirmation — see §15*)
- **Reliability:** The campaign execution engine **MUST** degrade gracefully if Communication Hub is temporarily unavailable — steps should be queued rather than dropped. Availability targets to be aligned with platform SLA. (*availability target needs confirmation — see §15*)
- **Scalability:** Campaign Manager **MUST** support multi-practice, multi-tenant operation. Audience segmentation queries must remain performant as the shared data model scales across practices. No practice's campaign activity may affect another practice's execution.
- **Security:** All campaign data, including audience snapshots and content references, **MUST** be encrypted at rest and in transit. Secrets and credentials used in integration contracts **MUST** be managed via the platform secrets management approach and **MUST NOT** be embedded in builder schemas.
- **Privacy:** Campaign Manager **MUST** honour GDPR subject rights (access, erasure, rectification) as they apply to marketing consent records and enrolment history. Data retention for campaign analytics and audience snapshots must align with the platform-level retention policy. No personal data may be duplicated into a local Campaign Manager store. Marketing is opt-in by default. Channel-specific opt-outs are enforced per Campaign Step. Unsubscribe and STOP events are processed centrally. Suppressed sends **MUST** be logged with explicit reason codes. All consent decisions are immutable and inspection-ready.
- **Observability:** Campaign Manager **MUST** export metrics covering campaign activation rate, enrolment volume, suppression event frequency, step execution latency, and AI suggestion acceptance rate. Structured logs **MUST** be emitted for all state transitions and integration events. Distributed traces **MUST** be available across the Campaign Manager → Communication Hub execution path.

15. Open Questions

1. **Approval model for campaign activation:** Must the activating user be different from the campaign creator, and is a single-operator practice exemption required? The current spec does not define this constraint.
2. **MFA requirements for sensitive operations:** Which specific campaign operations (e.g. bulk activation, consent-rule override) require MFA, and is this configured at the platform level in Access Manager or per-practice?

3. **Performance and availability targets:** Specific latency thresholds for suppression processing and availability SLA targets are not defined in the original spec and must be established before build.
4. **Tablet app surface:** The original spec does not define how Campaign Manager appears on the in-practice tablet. This needs definition before build.
5. **eligible_campaign_types[] values:** The normative event contract specifies this field as an advisory hint from Treatment Pipeline Manager, but the permitted enum values are not defined. These must be agreed between the Treatment Pipeline Manager and Campaign Manager teams.
6. **Cold threshold configuration:** The `pipeline.lead.cold` event is emitted when a Lead has received no qualifying activity within "the configured cold threshold" — where is this threshold configured, by whom, and does Campaign Manager have any visibility into it?
7. **Emergency stack identification:** The `source_channel` field is used to enforce emergency exclusion, but the full set of values that constitute an "emergency stack" is not enumerated. Engineering needs a complete list to implement the exclusion correctly.
8. **Concierge-hold timeout:** The configurable timeout period that governs how long Campaign Manager suppresses a contact following a concierge recovery-workflow signal (§4.2) must be defined; its default value and whether it is configurable at practice or platform level needs confirmation.
9. **Recall & Reconnect exit event schema:** The event name and payload fields for the Recall & Reconnect journey-completion and patient-exit events (used to lift suppression per §4.3) are not yet defined. These must be agreed with the Recall & Reconnect team before build.
10. **Loyalty Insights handoff signal schema:** The specific event names and payload fields for Loyalty Insights structured handoff signals (§4.4) are not yet defined and must be agreed before build.

16. Versioning & Governance

This specification is owned by: *(role to be confirmed)*

Changes to this spec require:

- Review by the Post-MVP module owner
- Impact analysis across all declared related modules (see /propose)
- Version bump (patch / minor / major as appropriate)

17. Build Contract (Engineering & QA)

17.1 Canonical Data Model

(Detailed schema to be defined at build. The following objects must be modelled: Campaign, CampaignStep, Journey, CampaignTemplate, BuilderSchema, AudienceSnapshot, EnrolmentRecord, SuppressionEvent, AuditEvent.)

17.2 Core Behaviour Rules

1. No Campaign may transition to Active state without explicit human activation by a user with Approve permission.
2. No Campaign Step may send a message directly; all delivery is delegated to Communication Hub via event.

3. On receipt of a suppression event (booking, opportunity closure, consent revocation, Recall & Reconnect enrolment, AI Concierge recovery-workflow hold), enrolment MUST halt before any subsequent Campaign Step executes.
4. Emergency stack contacts (`source_channel` identifying an emergency pipeline) MUST be excluded from nurture, keep-informed, and drip campaign types at the engine level; this exclusion MUST NOT be overridable by campaign configuration. Suppression of emergency stack contacts persists until a terminal pipeline resolution event is received, regardless of the 72-hour Emergency Stack record lifetime.
5. Builder Engine output MUST be entirely declarative (structured schema); no executable code may be persisted as campaign configuration.
6. All AI (Aiden) output is created in Draft state; no AI action may result in an Active campaign, an enrolment, or a message send.
7. Audience membership MUST be evaluated at send time, not at campaign creation time.
8. Contact fatigue constraints declared by Campaign Manager MUST be passed to Communication Hub and MUST NOT be bypassed at any layer.
9. AI Concierge signals MUST be consumed read-only; no Campaign Manager action may mutate concierge state.
10. All audit events listed in §8 MUST be written before the operation they record is considered complete.
11. Recall & Reconnect enrolment events MUST trigger suppression of conflicting campaign types for the enrolled patient; suppression MUST be lifted only upon receipt of a Recall & Reconnect exit or journey-completion event.
12. AI Quality Monitor data MUST NOT be used as an input to audience segmentation, suppression rules, or any campaign-targeting logic.

17.3 Configuration Surfaces

- **Practice-level settings (Admin Control Plane):** cold threshold, contact fatigue defaults, emergency stack identifiers, consent opt-in defaults, concierge-hold timeout
- **Per-campaign overrides (Campaign Manager Builder):** frequency caps, channel intent and fallback order, entry/exit/suppression conditions
- **Per-user preferences (Access Manager):** role-based access to create, edit, activate, and delete campaigns

17.4 Filtering & Views

The UI MUST support the following standard filters and views on the campaign dashboard:

- Filter by CampaignState (Draft / Scheduled / Active / Paused / Completed / Cancelled)
- Filter by campaign type (one-off / scheduled / dynamic)
- Filter by date range (created, activated, completed)
- Filter by AI-generated vs manually created campaigns
- Engagement metrics view per Campaign Step
- Attribution view linking campaigns to appointments booked, Opportunities progressed, and revenue recorded

17.5 Module Extension Map

- Pre-defined Campaign Templates are designed to be extended with new template types without altering the Builder Engine schema.
- The event subscription model (§4.1) is designed for additive extension; new source modules may be added as subscribers without modifying existing contracts.
- The `eligible_campaign_types[]` advisory field allows Treatment Pipeline Manager to signal new campaign type eligibility without requiring Campaign Manager schema changes, provided the new types are registered in Campaign Manager's configuration.

17.6 Acceptance Criteria

The build of Campaign Manager is complete when:

- [] All canonical objects (Campaign, CampaignStep, Journey, CampaignTemplate, BuilderSchema) can be created, read, and updated through the API
- [] Campaign state machine transitions enforce all rules in §3.2
- [] Builder Engine produces declarative, auditable schemas and rejects invalid or unsafe flows
- [] All inbound event subscriptions in §11.1 are wired and tested, including suppression events
- [] Emergency stack exclusion is enforced at engine level and cannot be overridden by configuration
- [] Recall & Reconnect enrolment suppression is enforced and lifted correctly on exit events (§4.3)
- [] AI Concierge recovery-workflow suppression hold is applied and released correctly (§4.2)
- [] Loyalty Insights handoff collision prevention is implemented per §4.4
- [] Care Plan Subscriptions inbound and outbound signals are wired per §4.5
- [] All outbound integration contracts in §11.2 are wired
- [] AI (Aiden) boundaries in §7 are enforced (negative tests pass: no auto-activation, no auto-enrolment, no auto-send, no AI Quality Monitor data ingestion)
- [] Audit log captures every event in §8, including all new suppression reason codes
- [] Access control is enforced per §9
- [] Contact fatigue constraints are declared and passed to Communication Hub correctly
- [] All non-functional requirements in §14 are met (with targets confirmed per §15)