Integrated Payments

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

Integrated Payments – Technical Specification

1. Module Purpose & Scope (Authoritative)

Integrated Payments provides a platform-native payments layer embedded inside Primoro, enabling practices to take payments in-practice, online, in the app, or by phone — with receipts, reconciliation, and audit trails built in. It exists to eliminate double entry between terminals, portals, and the PMS; insecure phone-payment workarounds; and disconnected receipts and inconsistent payment messaging.

Provider Model (Locked):

- Card & one-off payments: **DNA Payments** (UK acquirer; KYC handled by provider)
- Subscriptions / Direct Debit: **GoCardless** (subscription modules own collection; Integrated Payments surfaces status and exceptions only)

It governs:

- Payment execution across all surfaces: in-practice terminal, online/in-app, pay-by-link, and virtual terminal (phone/remote)
- Refunds, voids, and split payments with reason codes and audit trail
- Payment messaging and receipts, via Communication Hub
- Exception handling for failed payments, disputes, and overdue balances
- PMS writeback of payment and refund outcomes (near-real-time where supported; fallback tasks where not)
- Subscription payment status visibility and exception surfacing (collection remains GoCardless + subscription modules)
- Rewards credit application at checkout when Rewards Manager is enabled
- Financial Signal emission to Financial Insights for revenue attribution and reconciliation

It explicitly does not:

- Own deposit policy rules (owned by Appointment Manager)
- Own Direct Debit mandate creation, collection, retries, or mandate control (owned by GoCardless via the relevant subscription modules)
- Own lending or finance underwriting decisions (third-party finance providers)
- Store raw card data — PAN/CVV — at any point (tokenised/hosted entry only)
- Own reward credit eligibility rules or credit balance management (owned by Rewards Manager)

---

2. Ownership & Responsibilities

2.1 Integrated Payments IS Responsible For

- **Payment execution surfaces:** in-practice terminal payments initiated from Primoro; online/in-app payments (including digital wallets where supported); pay-by-link issuance and tracking; secure virtual terminal for phone/remote payments (RBAC-restricted).
- **Operational controls:** refunds, voids, and split payments with reason codes and audit trail; exception handling producing tasks and alerts on failure.
- **Payment messaging and receipts:** delivery via Communication Hub (app-first; email/SMS fallback); all communications logged.
- **PMS writeback:** posting successful payments and refunds to the PMS in near-real-time where supported; creating fallback tasks when provider or PMS writeback fails. GoCardless transaction fee data for subscription payments MUST be included in writeback payloads where direct PMS writeback is supported; where it is not, a fallback task MUST be created containing the fee detail for manual reconciliation by Finance Module.
- **Subscription status visibility:** surfacing subscription payment status and exceptions for Care Plan and Hygiene subscription flows; a Failed subscription payment status MUST be surfaced without delay so that downstream fulfilment modules can gate accordingly.
- **Rewards credit application at checkout:** when Rewards Manager is enabled, applying available reward credits automatically at checkout, reducing the amount charged to the primary payment method; recording the credit applied; reflecting it in the receipt; and emitting a redemption event back to Rewards Manager on successful capture.
- **Financial Signal emission:** emitting structured Financial Signal events to Financial Insights in near-real-time on the triggers defined in §7.3.
- **AI Guardian state interface:** exposing all lifecycle and subscription states as read-only signals to AI Guardian, containing state and metadata only — no card data, tokenised card references, or PAN-adjacent data.
- **Full auditability:** every payment, refund, void, override, approval, and rewards credit application is attributable to a named actor and immutably logged.

2.2 Integrated Payments IS NOT Responsible For

- Deposit policy rules — owned by **Appointment Manager**
- Direct Debit mandate creation, collections, retries, and mandate control — owned by **GoCardless** via the subscription modules (**Care Plan Subscriptions**, **Hygiene Subscriptions**)
- Lending or finance underwriting decisions — owned by third-party finance providers
- Raw card data storage — prohibited by construction; card entry is tokenised/hosted
- Reward credit eligibility rules and credit balance management — owned by **Rewards Manager**
- Subscription benefit fulfilment gating decisions — owned by **Care Plan Subscriptions** and **Hygiene Subscriptions** (Integrated Payments surfaces the status they act on)

---

3. Core Objects (Normative)

3.1 Payment (Canonical Artefact)

A Payment is a governed digital artefact representing a single payment interaction, from proposal through to reconciliation.

Every Payment MUST:

- be linked to a patient (or prospect where permitted)
- be linked to a valid billable target — valid types: invoice, patient balance, deposit, payment request, or commerce order (product purchase)
- A PMS invoice reference MAY be absent where the billable target is a commerce order originating from Product Shop; in such cases the payment is linked to the product order and a PMS invoice reference MAY be populated after fulfilment
- carry a provider reference ID (DNA Payments or GoCardless)
- carry a lifecycle state (see §3.2)
- be attributable to a named staff member (staff-initiated) or authenticated patient (self-serve)
- carry an immutable audit trail

3.2 Payment Lifecycle State Machine (Authoritative)

States:

- **Proposed** — amount known, payment not yet initiated
- **Initiated** — payment request created
- **Awaiting Customer Action** — terminal prompt issued / hosted checkout presented / pay-by-link sent
- **Authorised** — provider has authorised the transaction
- **Captured** — funds captured and confirmed
- **Failed** — declined or timed out
- **Partially Refunded** — captured payment has been partially refunded
- **Refunded** — full refund processed
- **Voided / Cancelled** — payment cancelled before capture
- **Reconciled** — matched into a payout batch

Rules:

- State transitions MUST be auditable and time-stamped.
- Only **Captured** payments may be written to the PMS as paid (unless the PMS supports a "pending" marker).
- Refunds MUST always reference the original transaction and original payment method, with a mandatory reason code.
- A payment MUST NOT return to Proposed or Initiated once it has reached Authorised or beyond.
- Provider timeouts MUST surface as **Failed** with a retry path available; duplicate capture MUST be prevented.

3.3 Subscription Status Model (Visibility Only — Authoritative)

Integrated Payments surfaces the following subscription payment states, sourced from GoCardless:

- Active mandate
- Payment pending
- Paid

- Failed
- Cancelled

Collection, retries, and mandate control remain GoCardless and the relevant subscription modules. A **Failed** status MUST be surfaced without delay; Care Plan Subscriptions and Hygiene Subscriptions act on this state to gate fulfilment.

3.4 Subscription Billing Boundary and Mandate References (Authoritative)

Integrated Payments does not own, initiate, or retry Direct Debit collections for subscription plans. Care Plan Subscriptions and Hygiene Subscriptions each own their respective Direct Debit billing lifecycle in full, including mandate creation, collection scheduling, retry logic, and mandate cancellation — all executed via GoCardless.

Where GoCardless subscription payments are referenced within Integrated Payments (for status surfacing, fee-data writeback, and Financial Signal emission), the following apply:

- A **PaymentMandateRef** — the GoCardless mandate reference associated with the subscription — MUST be carried on the payment status record that Integrated Payments surfaces. This reference is sourced from GoCardless via webhook/API and MUST NOT be generated or modified by Integrated Payments.
- Integrated Payments MUST NOT initiate a new Direct Debit collection for a subscription plan renewal or retry. Any such initiation is owned exclusively by Care Plan Subscriptions or Hygiene Subscriptions and is executed via GoCardless directly.
- Where a subscription payment status record is updated (e.g. from Payment pending to Paid or Failed), Integrated Payments MUST update its surfaced state and emit the relevant Financial Signal event without delay, but MUST NOT take any collection action as a result.
- The PaymentMandateRef MUST be included in the audit trail entry for every subscription payment status change surfaced by Integrated Payments, enabling end-to-end traceability from the GoCardless mandate through to PMS writeback and Financial Insights reconciliation.

This boundary ensures that Integrated Payments and the subscription modules cannot produce duplicate payment initiations. Any integration between these modules MUST be uni-directional for collection: the subscription module instructs GoCardless; GoCardless notifies Integrated Payments of outcomes; Integrated Payments surfaces status and emits signals.

---

4. Payment Execution Capabilities

4.1 In-Practice Terminal Payments

The module MUST:

- Allow staff to initiate a terminal payment from the patient account, appointment, or invoice context via the Payment Drawer.
- Send the amount to a staff-selected registered terminal (countertop or handheld) for the practice/site.
- Display an **Awaiting Customer Action** state in the UI until the terminal interaction is complete.
- Return and persist success or failure status from the terminal, and trigger receipt delivery via Communication Hub.

The module MAY:

- Support multiple registered terminals per site, with staff selecting the target terminal.

The module MUST NOT:

- Accept raw card entry on the tablet or staff web portal UI — card entry is patient-facing hardware only.

4.2 Online, In-App, and Pay-By-Link Payments (Authoritative)

The module MUST:

- Support patient-initiated payment of outstanding balances via the patient app.
- Issue pay-by-link URLs that are invoice-specific; deliver them via Communication Hub (push-first; email/SMS fallback).
- Handle pay-by-link completion and update both Primoro and the PMS without double entry.
- Support digital wallets where the provider supports them.

4.3 Virtual Terminal — Phone and Remote (Authoritative)

The module MUST:

- Restrict virtual terminal access by RBAC role.
- Use hosted or tokenised card entry — no raw card data stored.
- Emit a call-recording mute indicator during card entry when the Telephony / AI Receptionist module is enabled and supported by the telephony integration.

4.4 Refunds, Voids, and Split Payments (Authoritative)

The module MUST:

- Support full and partial refunds referencing the original transaction and method, with a mandatory reason code.
- Support void / cancellation before capture.
- Support split payment tenders (e.g. card + cash + voucher), preventing under-payment and over-payment, producing multiple ledger entries and a single settled outcome.
- Apply an optional approval workflow by role for high-value or high-risk refund actions.

4.5 Rewards Credit Application at Checkout

The module MUST:

- When Rewards Manager is enabled, apply the credit amount and redemption reference passed by Rewards Manager prior to capture, reducing the charge to the primary payment method.
- Record the credit applied against the transaction record.
- Reflect the credit in the patient-facing receipt.
- Emit a redemption event back to Rewards Manager on successful capture.

The module MUST NOT:

- Own reward eligibility logic, credit calculation, or balance management — those are Rewards Manager's responsibility.

4.6 System-Initiated Payment Triggers

The module MUST handle the following system-initiated triggers as valid payment sources:

- **Appointment Manager deposit collection events** — Appointment Manager enforces deposit policy; Integrated Payments executes collection and records outcomes.
- **Smart Treatment Proposals acceptance events** — when a patient accepts a proposal carrying a PaymentProfileID and a selected payment or finance option, Integrated Payments MUST use the PaymentProfileID to pre-populate the payment method and apply the selected option (deposit, staged payments, or finance referral). Finance referral routes to the relevant third-party provider; Integrated Payments records the outcome.
- **Admin Control Plane (ACP) Finance Centre billing events** — mandate management, payment retries, dunning sequences, and usage-based charges orchestrated by the ACP Finance Centre via GoCardless and DNA Payments MUST be handled as valid system-initiated triggers; outcomes MUST be reflected in the payment lifecycle and audit trail.

---

5. Delivery Surfaces & Access (Authoritative)

5.1 Web Portal — Primary Staff Workspace

Payment Drawer (patient / appointment / invoice context) MUST include:

- Amount selector: invoice total, partial, or custom amount
- Method selector: terminal / pay-by-link / virtual terminal (RBAC-controlled)
- Provider status panel: Initiated → Authorised → Captured / Failed
- Receipt preview and "Send receipt" (app-first) status indicator
- Audit panel: actor, timestamp, action, and provider reference

Terminal Selection and Control:

- Staff selects a registered terminal for the practice/site.
- UI displays **Awaiting Customer Action** until terminal interaction completes.

Refund / Void Flow:

- Full or partial refund; mandatory reason code; optional role-based approval workflow.

Split Payment Flow:

- Multiple tenders; under/over-payment prevention; multiple ledger entries with a single settled outcome.

Pay-By-Link Composer:

- Invoice-specific links; delivered via Communication Hub.

Virtual Terminal:

- RBAC-restricted; hosted/tokenised entry; call-recording mute indicator when Telephony / AI Receptionist is enabled.

5.2 Tablet App

The tablet is not a payment processor. It MAY:

- Initiate "collect payment" flows (routing to the terminal or link flow).
- Display payment status.

It MUST NOT:

- Accept raw card entry.

The terminal remains the patient-facing hardware for card-present payments.

5.3 Patient Mobile App

MUST include:

- Outstanding balances list
- "Pay now" action (balance or requested amount)
- Receipt history (app-first)
- Pay-by-link handling (one-time)

5.4 Engagement Signals

- Payment status badges in appointment and patient account views
- Exception banners for failed payments and disputes
- Tasks and alerts for follow-up and approvals
- Reconciliation indicators surfaced in dashboards where Financial Insights is enabled

---

6. Integration Contracts

6.1 Inbound (this module consumes from)

From module	What	Contract
Appointment Manager	Deposit collection trigger events	Event (system-initiated)
Rewards Manager	Applicable credit amount and redemption reference, pre-capture	Sync call before capture
Smart Treatment Proposals	Proposal acceptance event with PaymentProfileID and selected payment option	Event (system-initiated)
ACP Finance Centre	Billing orchestration events (mandates, retries, dunning, usage charges)	Event (system-initiated)
GoCardless	Subscription payment status, mandate references (PaymentMandateRef), and transaction fee data	Webhook / API

DNA Payments	Card transaction authorisation and capture outcomes	Webhook / API
Inventory & Compliance Manager	Purchase-order invoice verification signals where PO-to-invoice reconciliation requires confirmation of payment execution	Event (async, best-effort)

6.2 Outbound (this module emits to)

To module	What	Contract
Communication Hub	Receipt delivery triggers; pay-by-link delivery; all payment communication logs	Event
Task Manager	Tasks for failed payments, exceptions, fallback writeback, approvals	Event
Financial Insights	Financial Signal events (payment.captured, payment.refunded, payment.partially_refunded, deposit.converted, deposit.forfeited, subscription.payment.received, subscription.payment.failed)	Near-real-time event stream
Rewards Manager	Redemption event on successful capture	Event
AI Guardian	Read-only payment and subscription lifecycle state signals (state + metadata; no card data)	Read-only signal interface
Finance Module	GoCardless fee data via PMS writeback payload or fallback task	Sync writeback / async task
Care Plan Subscriptions	Failed subscription payment status (consumed to gate fulfilment)	Event / state signal
Hygiene Subscriptions	Failed subscription payment status (consumed to gate fulfilment)	Event / state signal

PMS	Payment and refund writeback, including fee data where applicable	Near-real-time sync; fallback task
Inventory & Compliance Manager	Payment execution confirmation for matched purchase-order invoices, to support PO-to-invoice reconciliation	Event (async, best-effort)

6.3 PMS Boundary

The PMS is the record of invoices and patient accounts. Integrated Payments is the record of payment execution. The boundary is:

- The PMS presents the billable target (invoice, patient balance); Integrated Payments executes the payment and writes the outcome back.
- Only **Captured** payments are written to the PMS as paid (unless the PMS supports a "pending" marker).
- Where PMS writeback is not supported or fails, Integrated Payments creates a fallback task for manual reconciliation, including GoCardless fee data where applicable.
- Integrated Payments does not create or modify PMS invoices; it references them.

6.4 Inventory & Compliance Manager Boundary

Inventory & Compliance Manager manages the procurement lifecycle — including goods-received confirmation and purchase-order invoice matching — but does not act as an accounting system. Where a matched supplier invoice requires payment execution (e.g. a practice paying a supplier), the handoff to Integrated Payments is as follows:

- Inventory & Compliance Manager signals that a purchase order has been matched to a verified supplier invoice and that payment execution is required. This signal is consumed by Integrated Payments as a system-initiated trigger.
- Integrated Payments executes and records the payment, then emits a confirmation event back to Inventory & Compliance Manager so that the procurement record can be marked as paid and reconciled.
- Integrated Payments does not own PO matching logic, supplier invoice verification, or goods-received confirmation — these remain Inventory & Compliance Manager's responsibility.
- This integration is scoped to practice-side procurement payments only and does not affect the patient payment lifecycle.

---

7. AI Boundaries (Non-Negotiable)

AI MAY:

- Summarise payment activity for human staff review.
- Explain payment options to patients or staff.

AI MAY NOT:

- Initiate, modify, or cancel any payment, refund, or void.

- Access card data, tokenised card references, or any PAN-adjacent data — by construction, these are never included in AI-accessible signals.
- Bypass RBAC controls, audit requirements, or governance checks.
- Make payment commitments on behalf of the practice.

AI Guardian reads payment and subscription lifecycle state signals from Integrated Payments as part of its platform-wide audit function. This interface is read-only from AI Guardian's perspective. Integrated Payments MUST expose all lifecycle states defined in §3.2 and §3.3 as derived signals to AI Guardian. These signals MUST contain only state and metadata (amount, state transition, timestamp, site/terminal ID, provider reference). Card data, tokenised card references, and any PAN-adjacent data MUST NEVER be included.

---

8. Audit & Compliance

The system MUST log (immutably):

- Who initiated each action — named staff member or authenticated patient
- When (UTC timestamp)
- Where — site ID and terminal ID where applicable
- What — amount, payment method, billable target type and reference
- Provider reference IDs (DNA Payments or GoCardless)
- All lifecycle state transitions and their outcomes
- Refunds and voids, including reason code and approver identity for role-restricted actions
- Overrides and approvals with approver identity
- Rewards credit applied — amount and redemption reference, where applicable
- All payment communications (links, receipts) — logged in Communication Hub
- PaymentMandateRef for all subscription payment status changes surfaced from GoCardless

Audit logs MUST be immutable and exportable for compliance inspection.

The following are the specific audit events Integrated Payments emits: - `payment.initiated` — actor, amount, method, billable target, timestamp - `payment.state_changed` — from-state, to-state, actor, provider reference, timestamp - `payment.refunded` / `payment.partially_refunded` — amount, original transaction reference, reason code, approver (if applicable), timestamp - `payment.voided` — actor, reason code, approver (if applicable), timestamp - `rewards_credit.applied` — credit amount, redemption reference, transaction reference, timestamp - `pms_writeback.failed` — transaction reference, failure reason, fallback task ID, timestamp - `approval.required` / `approval.granted` / `approval.denied` — action type, actor, approver, timestamp - `subscription.payment.status_changed` — PaymentMandateRef, from-state, to-state, provider reference, timestamp

---

9. Access Control

Access control is governed by Access Manager. The following role-based permissions apply:

Action	Who may perform

Initiate terminal / online payment	Authorised staff (standard role)
Issue pay-by-link	Authorised staff (standard role)
Use virtual terminal	RBAC-restricted role only
Issue refund / void	RBAC-restricted role; high-value actions may require an approver
Approve high-value refund	Designated approver role
View payment history	Authorised staff; patient (own records only via app)
View audit log	Compliance / admin role

MFA requirements for virtual terminal access and high-value refund approval are subject to the Access Manager configuration; the Access Manager spec governs MFA policy platform-wide.

---

10. Integration Summary

- **DNA Payments** — primary payment provider; card acquiring, KYC, payouts (inbound outcomes via webhook/API)
- **GoCardless** — Direct Debit provider; subscription payment status, mandate references (PaymentMandateRef), and fee data (inbound via webhook/API)
- **Appointment Manager** — inbound deposit collection trigger events
- **Communication Hub** — outbound receipt and pay-by-link delivery; all payment communication logs
- **Task Manager** — outbound tasks for failures, exceptions, fallback writeback, approvals
- **Financial Insights** — outbound Financial Signal events (near-real-time event stream)
- **Rewards Manager** — inbound credit amount and redemption reference pre-capture; outbound redemption event on capture
- **Smart Treatment Proposals** — inbound proposal acceptance events triggering payment or plan setup
- **ACP Finance Centre** — inbound billing orchestration events (mandates, retries, dunning, usage charges)
- **AI Guardian** — read-only outbound state signal interface; no card data
- **Finance Module** — GoCardless fee data via PMS writeback payload or fallback task
- **Care Plan Subscriptions** — outbound failed subscription payment status signal; subscription billing collection owned exclusively by Care Plan Subscriptions via GoCardless
- **Hygiene Subscriptions** — outbound failed subscription payment status signal; subscription billing collection owned exclusively by Hygiene Subscriptions via GoCardless
- **Access Manager** — RBAC for all role-restricted operations
- **PMS** — near-real-time payment and refund writeback; fallback task on failure
- **Product Shop** — commerce order as a valid billable target type
- **Inventory & Compliance Manager** — inbound PO invoice verification signals; outbound payment execution confirmation for matched supplier invoices

11. Explicit Non-Goals

- **Deposit policy enforcement** — policy is owned and enforced by Appointment Manager; Integrated Payments executes collection only.
- **Direct Debit mandate creation, collections, and retries** — owned by GoCardless via Care Plan Subscriptions and Hygiene Subscriptions; Integrated Payments surfaces status and emits signals only and MUST NOT initiate or retry any Direct Debit collection on behalf of a subscription module.
- **Lending and finance underwriting** — owned by third-party finance providers; Integrated Payments records referral outcomes only.
- **Raw card data storage** — prohibited by construction; not a deferred goal.
- **Reward eligibility logic and credit balance management** — owned by Rewards Manager.
- **Subscription benefit fulfilment gating** — owned by Care Plan Subscriptions and Hygiene Subscriptions; Integrated Payments provides the status signal they act on.
- **Purchase-order matching and supplier invoice verification** — owned by Inventory & Compliance Manager; Integrated Payments executes and confirms payment only.

12. Versioning & Governance

This specification is owned by: *(no content captured in original — needs definition)*

Changes to this spec require:

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

13. Build Contract (Engineering & QA)

13.1 Canonical Data Model

(no schema captured in original — needs definition by engineering)

Minimum required fields on the Payment record:

- PaymentID (UUID, primary key)
- PatientID (FK — or ProspectID where permitted)
- BillableTargetType (enum: invoice | patient_balance | deposit | payment_request | commerce_order)
- BillableTargetID (FK to the relevant billable target)
- ProviderReferenceID (string — DNA Payments or GoCardless reference)
- LifecycleState (enum: see §3.2)
- InitiatedBy (UserID or "patient-self-serve")
- SiteID
- TerminalID (nullable)

- Amount (decimal, currency)
- RewardsCreditApplied (decimal, nullable)
- RewardsCreditRedemptionReference (string, nullable)
- PaymentMandateRef (string, nullable — GoCardless mandate reference; populated for subscription payment status records only)
- CreatedAt (UTC timestamp)
- UpdatedAt (UTC timestamp)
- AuditTrail (immutable append-only log)

13.2 Core Behaviour Rules

1. Every payment MUST be linked to a patient (or prospect) and a valid billable target before it can be initiated.

2. A PMS invoice reference MAY be absent where the billable target is a commerce order from Product Shop; the payment is linked to the product order.

3. Only Captured payments may be written to the PMS as paid (unless the PMS supports a "pending" marker).

4. Refunds MUST reference the original transaction and original payment method; a reason code is mandatory.

5. Duplicate capture MUST be prevented; provider timeouts MUST surface as Failed with a retry path.

6. Failed payments MUST create a task and/or alert; silent failures are prohibited.

7. Virtual terminal access MUST be RBAC-restricted; no raw card data is stored at any point.

8. Phone payments MUST mute call recording during card entry when the Telephony / AI Receptionist module is enabled and supported.

9. Rewards credit MUST be applied only when Rewards Manager passes a valid credit amount and redemption reference prior to capture; Integrated Payments does not calculate eligibility.

10. A Failed subscription payment status MUST be surfaced without delay; Care Plan Subscriptions and Hygiene Subscriptions rely on this state to gate fulfilment.

11. Payment state signals exposed to AI Guardian MUST never contain card data, tokenised card references, or PAN-adjacent data.

12. Financial Signal events MUST be emitted within the same near-real-time window as PMS writeback.

13. GoCardless fee data MUST be included in PMS writeback payloads for subscription payments; where writeback is not available, a fallback task containing the fee detail MUST be created for Finance Module reconciliation.

14. ACP Finance Centre billing orchestration events MUST be reflected in the payment lifecycle and audit trail.

15. Smart Treatment Proposal acceptance events MUST pre-populate the payment method using the supplied PaymentProfileID and apply the selected payment option.

16. Integrated Payments MUST NOT initiate, schedule, or retry any Direct Debit collection for a subscription plan; collection is owned exclusively by Care Plan Subscriptions or Hygiene Subscriptions via GoCardless. Any subscription payment status update received from GoCardless MUST be surfaced and signal-emitted only.

17. A PaymentMandateRef MUST be carried on every subscription payment status record surfaced by Integrated Payments and MUST be included in the audit trail entry for every associated status change.

18. Where Inventory & Compliance Manager signals that a matched purchase-order invoice requires payment execution, Integrated Payments MUST treat this as a valid system-initiated trigger, execute and record the payment, and emit a confirmation event back to Inventory & Compliance Manager.

13.3 Configuration Surfaces

- **Practice-level settings (Admin Control Plane):** registered terminals per site; virtual terminal enablement; approval thresholds for high-value refunds; GoCardless / DNA Payments provider credentials.
- **Per-user preferences (Access Manager):** role assignment for RBAC-restricted operations (virtual terminal, high-value refunds).
- **Per-payment overrides:** split payment tenders; partial refund amounts; reason code selection.

13.4 Filtering & Views

The following standard filters and views MUST be supported in the staff web portal:

- Filter payments by: date range, site, staff member, payment method, lifecycle state, billable target type
- Filter by exception type: failed payments, pending reconciliation, pending PMS writeback
- Subscription payment view: status by patient, by subscription module
- Refund and void log: filterable by actor, date range, reason code

13.5 Module Extension Map

- Digital wallet support may be extended per DNA Payments provider capability without breaking the payment lifecycle contract.
- Additional billable target types may be added to the BillableTargetType enum via a minor version bump with impact analysis.
- Additional Financial Signal event types may be added as new triggers emerge; Financial Insights consumers MUST be notified of new event types.
- Finance provider integrations for lending/underwriting referrals may be added as distinct integration surfaces without modifying the core payment lifecycle.

13.6 Acceptance Criteria

The build of Integrated Payments is complete when:

- [ ] Card-present terminal payments can be initiated from Primoro and return success/failure status, with receipts sent app-first via Communication Hub.
- [ ] Online/in-app payments and pay-by-link complete and update PMS and Primoro status without double entry.
- [ ] Virtual terminal payments are RBAC-restricted and do not store raw card data; call recording is muted during entry where Telephony / AI Receptionist is enabled.
- [ ] Refunds, voids, and split payments work end-to-end with reason codes and audit trail; optional approval workflow functions for high-value actions.
- [ ] Subscription Direct Debit collections remain GoCardless; Integrated Payments surfaces status and exceptions and creates tasks when failures occur; Failed subscription payment status is surfaced promptly and consumed correctly by Care Plan Subscriptions and Hygiene Subscriptions to gate fulfilment; Integrated Payments cannot initiate or retry any Direct Debit collection.

- [ ] All subscription payment status records surfaced by Integrated Payments carry the GoCardless PaymentMandateRef, and every status change is recorded in the audit trail with the mandate reference.
- [ ] All transactions are attributable, auditable, and visible in Communication Hub logs and dashboards where enabled.
- [ ] Rewards credit is applied at checkout when Rewards Manager passes a valid credit amount and redemption reference; the applied credit is recorded in the transaction record, reflected in the receipt, and a redemption event is returned to Rewards Manager on capture.
- [ ] Commerce order payments (Product Shop) are accepted as a valid billable target without requiring a PMS invoice reference; product orders are linked to the governed payment object correctly.
- [ ] Financial Signal events (`payment.captured`, `payment.refunded`, `payment.partially_refunded`, `deposit.converted`, `deposit.forfeited`, `subscription.payment.received`, `subscription.payment.failed`) are emitted in near-real-time and consumable by Financial Insights with correct `practice_id`, `patient_id`, and `billable_target` payloads.
- [ ] Payment state signals are accessible to AI Guardian for all lifecycle states defined in §3.2 and §3.3; no card data or tokenised card references are present in any exposed signal.
- [ ] Smart Treatment Proposals acceptance events correctly initiate payment or payment-plan setup flows using the supplied PaymentProfileID and selected payment option.
- [ ] ACP Finance Centre billing orchestration events (mandate management, retries, dunning, usage-based charges) are handled as valid system-initiated triggers and are reflected in the payment lifecycle and audit trail.
- [ ] GoCardless fee data for subscription payments is included in PMS writeback payloads (or fallback tasks) to support Finance Module reconciliation.
- [ ] Inventory & Compliance Manager PO invoice verification signals are handled as valid system-initiated payment triggers; payment execution confirmation events are emitted back to Inventory & Compliance Manager on capture.
- [ ] All state machine transitions enforce the rules in §3.2.
- [ ] All integrations in §6 are wired and tested.
- [ ] AI boundaries in §7 are enforced (negative tests pass — no card data in AI Guardian signals; AI Guardian cannot initiate or modify payments).
- [ ] Audit log captures every event in §8.
- [ ] Access control is enforced per §9.
- [ ] All non-functional requirements in §14 are met.

---

14. Non-Functional Requirements

- **Performance:** Real-time status feedback in staff UI for terminal and hosted payment flows. Financial Signal events MUST be emitted within the same near-real-time window as PMS writeback to ensure Financial Insights dashboards remain consistent with transaction state.
- **Reliability:** Provider timeouts MUST surface as Failed with a retry path; duplicate capture MUST be prevented. Fallback task creation for PMS writeback failures MUST be reliable; a failed writeback MUST never result in a silent gap in the audit trail.
- **Scalability:** The module MUST support multi-site, multi-terminal deployments within a single practice group, with site ID and terminal ID correctly attributed on all payment records and audit events.

- **Security:** PCI scope MUST be minimised via tokenisation and hosted card entry fields — no raw card data is stored by Primoro. RBAC enforced for virtual terminal and high-value refund operations. The AI Guardian state interface MUST be read-only and card-data-free by construction. All data in transit MUST be encrypted (TLS). All data at rest MUST be encrypted. Secrets and provider credentials MUST be managed via the platform secrets management capability and MUST NOT be stored in application configuration.
- **Privacy:** Patient payment data is subject to GDPR. The module MUST honour patient data subject access requests and right-to-erasure requests within the constraints of financial record retention obligations. Data retention policy for payment records MUST be defined in alignment with applicable financial regulations (no content captured in original — needs definition).
- **Observability:** The module MUST export metrics covering: payment success/failure rates by method and site; PMS writeback success/failure rates; Financial Signal emission latency; refund and void rates. All payment lifecycle state transitions MUST be traceable end-to-end. Structured logs MUST be emitted for all audit events defined in §8.
- **Accessibility:** Staff-facing UI surfaces MUST meet WCAG 2.1 AA accessibility standards. Patient-facing app surfaces are governed by the patient app's accessibility standard.

---

15. Open Questions

1. **Data retention policy for payment records:** What is the required retention period for payment records and audit logs, given applicable UK financial regulations? (Implicit in §14 Privacy — no definition captured in original.)
2. **PMS writeback "pending" marker support:** Which PMS integrations support a "pending" payment marker? The behaviour for Captured payments differs depending on this support — the list of supported PMS partners needs to be defined. (Implicit in §3.2 and §6.3.)
3. **Approval thresholds for high-value refunds:** What amount threshold triggers the optional approval workflow for refunds? Is this practice-configurable or platform-defined? (Implicit in §4.4 and §9.)
4. **Finance provider integrations for lending/underwriting:** Which third-party finance providers are in scope for the Smart Treatment Proposals finance-referral flow? The integration surface is declared but providers are not named. (Implicit in §4.6 and §2.2.)
5. **GoCardless fee data availability:** Is transaction fee data always available from the GoCardless API at the time of payment confirmation, or is it available only after settlement? This affects the timing of writeback payloads and fallback task content. (Implicit in §2.1.)
6. **Spec ownership:** Which role owns this specification and is responsible for approving changes? (Required for §12; not captured in original.)
7. **Inventory & Compliance Manager payment trigger scope:** Is the PO-to-invoice payment trigger limited to practice-side procurement (supplier payments), or does it extend to other invoice types? The integration in §6.4 assumes procurement-only scope; confirmation is needed before implementation. (Implicit in §6.4.)