Surgery & Decon Day View

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

Surgery & Decon Day View – Technical Specification

1. Module Purpose & Scope (Authoritative)

The Surgery & Decon Day View provides a nurse-first, real-time operational view for today's surgeries and decontamination work, making readiness, compliance, and required clinical context visible and actionable on shared tablets. It exists to surface today's schedule filtered to rota-assigned surgery and nurse context, to provide tray readiness signalling and decon work-package compliance tracking in real time, and to govern day-of execution while synchronising appointment progress back to the PMS (which remains the system of record). The module is the authoritative interface for named, attributable nurse action at point of work; it is not a planning, scheduling, or inventory system.

It governs:

- Today-only appointment visibility for nurses, filtered by rota assignment and nurse context
- Two distinct tablet surfaces with enforced separation of concerns: Decon Wall Tablet (awareness and compliance) and Surgery Tablet (action and completion)
- Tray readiness confirmation, in-chair workflow steps, and governed appointment completion via Finish & Send
- Decon daily/scheduled task (work package) surfacing, completion, and overdue signalling
- Fast, secure nurse login and user switching on shared devices (badge tap, PIN, QR fallback)

It explicitly does not:

- Own appointment booking rules or diary logic — governed by Appointment Manager
- Own staffing or coverage planning — governed by Rota Manager
- Define tasks, escalation policy, or task lifecycle transitions — governed by Task Manager; this module only surfaces and completes what Task Manager assigns
- Implement lab workflow management — Lab Manager is explicitly out of scope for MVP; only lab-required awareness signals are surfaced
- Provide instrument databases, kit lists, or treatment-code-to-kit mapping — explicitly excluded from MVP

2. Ownership & Responsibilities

2.1 Surgery & Decon Day View IS Responsible For

- Displaying today's rota-filtered appointment schedule on both tablet surfaces with mandatory clinical context fields (including tooth numbers)
- Enforcing separation of concerns between the Decon Wall Tablet (low-interaction, awareness and compliance) and the Surgery Tablet (high-interaction, action and completion)

- Recording tray readiness confirmations with nurse identity and timestamp (Surgery Tablet only)
- Surfacing Task Manager work packages with due time, status, completed-by attribution, and overdue highlighting on both surfaces
- Enforcing named, attributable sessions on shared devices — no anonymous or unattended usage is permitted
- Emitting audit log events for all authentication events, tray readiness confirmations, task completions, and in-chair completion markers
- Synchronising appointment progress back to the PMS via the declared integration contract

2.2 Surgery & Decon Day View IS NOT Responsible For

- Appointment booking logic or diary availability rules — owned by Appointment Manager
- Rota planning, coverage decisions, or shift scheduling — owned by Rota Manager
- Defining, creating, or driving task lifecycle transitions — owned by Task Manager
- Lab workflow automation or case management — owned by Lab Manager (future)
- Inventory, instrument, or consumable management — owned by Inventory & Compliance Manager (future)
- Emergency workflow logic — explicitly excluded from MVP scope
- Communications transport for notifications — owned by Communication Hub

3. Core Objects (Normative)

3.1 AppointmentDayRow (Canonical Read Artefact)

An AppointmentDayRow is a governed read-model artefact representing a single appointment surfaced to a tablet surface for a nurse's today-only, rota-filtered view.

Minimum required fields:

- AppointmentId
- StartTime
- SurgeryId / SurgeryName
- ClinicianId / ClinicianName
- AppointmentTypeId / AppointmentTypeName
- ToothNumbers[] (mandatory to display where available)
- LabRequired (bool)
- LabCaseReference (nullable)
- Notes (nullable)

`LabRequired` and `LabCaseReference` are appointment-level canonical properties sourced read-only from Lab Manager (when enabled) and from the Appointment Manager feed otherwise. Both fields are display-only on this module: they MUST NOT appear as write targets in TrayReadiness, WorkPackageTaskRow, or any other write surface. Where Lab Manager is not yet enabled, `LabRequired` and `LabCaseReference` are populated from the Appointment Manager feed and remain subject to the same read-only constraint.

3.2 TrayReadiness (Canonical Write Artefact — Surgery Tablet Only)

A TrayReadiness record is a governed write-model artefact representing a nurse's confirmation that a tray is prepared for a specific appointment.

Minimum required fields:

- AppointmentId
- TrayReady (bool)
- TrayReadyTimestamp
- TrayReadyByUserId

3.3 WorkPackageTaskRow (Canonical Read/Write Artefact)

A WorkPackageTaskRow is a governed artefact representing a decon compliance task assigned via Task Manager and surfaced on tablet views.

Minimum required fields:

- TaskId
- WorkPackageId
- TaskName
- DueTime
- Status
- CompletedTimestamp
- CompletedByUserId

3.4 SharedDeviceSession (Canonical Artefact)

A SharedDeviceSession is a governed artefact representing an authenticated nurse session on a shared tablet device.

Minimum required fields:

- DeviceId
- UserId
- AuthMethod (Badge | PIN | QR)
- LoginTimestamp
- LogoutTimestamp / TimeoutTimestamp

The SharedDeviceSession object in this module MUST conform to Access Manager's canonical session state machine and enforcement rules (Access Manager §4.2–4.3). Access Manager is the authoritative enforcement layer for session state; this module's local representation is a projection of that state and must not diverge from it. In particular:

- Session state transitions (active → timed-out, active → rota-end-terminated, active → explicit-logout) are governed by Access Manager; this module must honour and reflect those transitions faithfully.
- Between-user data wipe (see §4 below) is a non-negotiable control enforced at session boundary; any locally cached patient or appointment data must be cleared as part of session termination before a new session may begin.
- The module must not implement an alternative or supplementary session model that bypasses or duplicates Access Manager's enforcement.

3.5 WorkPackageTaskRow State Rendering (Authoritative)

Task Manager owns the governed task lifecycle: **Created** → **Active** → **In Progress** → **Blocked** → **Completed** → **Cancelled** → **Archived**. The Day View does not own or drive these transitions. The following rendering rules apply to each state on both tablet surfaces:

- **Active** — task is due and actionable; displayed in the normal work queue
- **In Progress** — task has been started but not completed; displayed with an in-progress indicator
- **Blocked** — task cannot proceed as signalled by Task Manager; must receive a distinct visual treatment (e.g. a blocked/warning indicator) so nurses are not silently left with an unactionable task
- **Completed** — displayed with completed-by attribution and timestamp; retained in view for the remainder of the day for audit and awareness purposes
- **Cancelled** — displayed with a cancelled state indicator; nurses must not be prompted to act on cancelled tasks
- **Created** and **Archived** states are internal to Task Manager and are not expected to surface directly on either tablet view

All status transitions remain owned by Task Manager and are auditable end-to-end; the Day View records completion events locally (nurse identity and timestamp) and these are reconciled back to Task Manager.

4. Tablet Surfaces & Workflow

4.1 Separation of Concerns (Non-Negotiable Design Principle)

The module operates across two tablet experiences. This separation is a non-negotiable design principle and must not be collapsed.

- **Decon Wall Tablet** — visibility and compliance; low interaction
- **Surgery Tablet** — action and completion; high interaction

4.1.1 Shared-Device Security Controls (Non-Negotiable)

Both tablet surfaces operate on shared clinic devices and MUST comply with Security & Privacy platform requirements (Security & Privacy §4.3). The following controls are non-optional:

- **Mandatory authentication before session start** — no content may be displayed, and no interaction is possible, before a named nurse has authenticated. This applies on initial device wake, after any session timeout, and after any explicit logout.
- **Auto-logout** is triggered by two independent conditions, whichever occurs first: (a) inactivity timeout as configured in Admin device policy, and (b) rota end time as supplied by Rota Manager. Both triggers must be enforced independently; disabling one must not disable the other.
- **Full data wipe between users** — on session termination (by any trigger), all locally cached patient-bound data, appointment data, and session credentials MUST be purged from device storage before the login surface is presented. A new session MUST NOT be able to access any data from the previous session.
- These controls apply equally to the Decon Wall Tablet and the Surgery Tablet; there is no surface on which a reduced security posture is permitted.

4.2 Decon Wall Tablet (Awareness & Compliance)

Purpose: a glanceable "what's happening / what's coming / what's missing" view. It must not become a per-appointment ticking surface; micro-task execution is explicitly excluded.

The module MUST:

- Display today-only appointments filtered by rota/nurse context
- Show for each appointment row: time, surgery, clinician, appointment type, tooth number(s), lab-required flag, and lab case reference (if present)
- Surface decon compliance work packages with due time, status, completed-by attribution, and overdue highlighting
- Visually flag overdue tasks with a distinct treatment

The module MAY:

- Emphasise the next four upcoming appointments prominently ("4-tray lookahead") to support advance preparation

The module MUST NOT:

- Surface appointment rows that are not backed by a valid Rota Entry from Rota Manager
- Display inferred or pattern-derived appointment slots

4.3 Surgery Tablet (Action & Completion) (Authoritative)

Purpose: where work is completed — tray readiness, in-chair workflow steps, forms and consents, and appointment completion.

The module MUST:

- Display an appointment header including: patient name, appointment type, tooth number(s), lab-required flag, lab case reference (if present), and notes (if present)
- Enable single-tap Tray Ready confirmation, recorded with nurse identity and timestamp
- Present governed in-chair workflow steps and enforce Finish & Send as the hard stop for appointment completion
- Surface form and consent status (complete / incomplete / blocked) in the appointment header or workflow step list so nurses can act before the clinician enters the surgery
- Block in-chair workflow progression when mandatory forms (as defined by Digital Forms) are missing or out of date; this blocking state must be visible to the nurse prior to and during the session
- Enforce a hard gate immediately before Finish & Send: if any mandatory form for the appointment is unsigned or incomplete as reported by Digital Forms, Finish & Send MUST be unavailable and the nurse MUST be shown a clear indication of which form(s) are blocking completion. This gate is non-negotiable and cannot be bypassed by any user role. Form status is queried from Digital Forms via the inbound read/sync contract declared in §6.1; the module must re-query or receive a push update from Digital Forms at the point the nurse attempts to initiate Finish & Send to ensure the gate reflects the current state
- Delegate all signature capture to Digital Forms' governed signing rules, including time-stamped, version-locked capture; no lightweight or informal signature path is permitted as a substitute

The module MUST NOT:

- Allow Tray Ready confirmation to be recorded without a named, authenticated nurse
- Allow in-chair workflow to proceed past a mandatory form gate until that form is satisfied

- Allow Finish & Send to complete while any mandatory form remains unsigned or incomplete, regardless of any other workflow state

4.4 "Now / Next" Time Awareness

Both views are designed to emphasise what is imminent and what needs action under time pressure. Filtering and view ordering must support "imminent/next" emphasis as the default day-of flow.

5. Delivery Surfaces & Access (Authoritative)

5.1 Web Portal

(no content captured in original — needs definition)

5.2 Tablet App

The primary delivery surface for this module is the shared tablet. Two distinct experiences are delivered:

- **Decon Wall Tablet** — wall-mounted, low-interaction, today-only schedule and decon compliance view
- **Surgery Tablet (Nurse View)** — high-interaction, tray readiness, in-chair workflow steps, and appointment completion surface

Both tablet surfaces must meet glove-friendly interaction requirements: large touch targets, minimal navigation depth, and fast view load times appropriate for day-of clinical operations.

5.3 Patient Mobile App

This module does not deliver a patient-facing surface.

5.4 Engagement Signals

- Overdue decon task counts visible to nurses on the Decon Wall Tablet
- Lab-required appointment flags visible on both surfaces
- Pre-session readiness signals (e.g. unreceipted lab cases) surfaced as distinct indicators when Lab Manager is enabled

6. Integration Contracts

6.1 Inbound (this module consumes from)

From Module	What	Contract
Appointment Manager	Today-only, rota-context-filtered appointment feed — appointment schedule and appointment metadata scoped to the authenticated nurse's rota assignment and the current date; see note below	Read / sync

Rota Manager	Day-of nurse rota assignments, shift windows, and break segments — consumed as a read-only feed; used to filter both tablet surfaces by rota-assigned surgery and nurse context, to validate appointment backing, and to supply rota end-time for automatic session termination	Read / sync
Task Manager	Decon compliance work packages with lifecycle state	Read / async
Digital Forms	Form completion status and mandatory form gate state — queried per appointment; re-queried or push-updated at the point Finish & Send is initiated to ensure gate reflects current state	Read / sync
Lab Manager	`LabRequired` flag and `LabCaseReference` per appointment, including unreceipted lab case status for pre-session readiness signalling (when Lab Manager is enabled)	Read / sync
PMS	Appointment record (system of record)	Read

Appointment Manager feed note: Appointment Manager publishes a today-only, rota-context-filtered appointment feed for operational downstream surfaces. For this module, that feed is scoped to the authenticated nurse's surgery and rota context and to the current date only. The feed is the authoritative source of AppointmentDayRow data; the module must not construct appointment rows from any other source. Update frequency and push/pull mechanism are to be confirmed (see Open Questions §15).

6.2 Outbound (this module emits to)

To Module	What	Contract
Task Manager	Task completion events (nurse identity + timestamp)	Event / async
PMS	Appointment progress synchronisation (Finish & Send)	Write / sync
Audit & Compliance	Immutable audit log events for all governed actions	Event

Digital Forms	Signature capture delegation (consent and forms in-chair)	Delegated write
Aftercare Manager	Aftercare delivery trigger from surgery workflow completion	Event

6.3 PMS Boundary

The PMS is the system of record for appointments. The Surgery & Decon Day View consumes appointment data from Appointment Manager (which reflects PMS state) and writes appointment progress back to the PMS via Finish & Send. The Day View does not own appointment records and must not modify appointment data outside the governed progress-synchronisation contract.

6.4 Lab Manager Integration Note

`LabRequired` and `LabCaseReference` are surfaced on both tablet surfaces as read-only appointment-level properties. At MVP, these values are sourced from the Appointment Manager feed. When Lab Manager is enabled, the inbound Lab Manager contract (§6.1) enriches these values with live lab case status and supplies the unreceipted-case pre-session readiness signal. In both cases, this module treats these fields as read-only display properties and must not write to or modify them.

7. AI Boundaries (Non-Negotiable)

This module does not embed AI surfaces directly in the MVP scope.

Should AI-assisted features (e.g. task prioritisation suggestions, readiness anomaly detection) be introduced in a future version, they must comply with platform-level AI governance: AI MAY suggest content for human review; AI MAY NOT auto-complete governed workflow steps, bypass audit requirements, or make clinical judgements on behalf of a nurse or clinician.

8. Audit & Compliance

The system MUST log the following events, each with actor identity and timestamp:

- Nurse authentication events — login, user switch, inactivity timeout, rota-end-time logout
- Tray Ready confirmations — nurse identity, appointment reference, timestamp
- Decon work package task completions — nurse identity, task reference, timestamp
- In-chair workflow step completions and Finish & Send events — nurse identity, appointment reference, timestamp
- Mandatory form gate events — when a gate is encountered and when it is satisfied
- All cross-module events emitted or consumed (task completion to Task Manager, Finish & Send to PMS, aftercare trigger to Aftercare Manager)

Audit logs MUST be immutable and exportable for inspection. No audit event may be deleted or amended by any user, including administrators.

Auditability and attributable actions are explicitly non-negotiable in the nurse tablet MVP.

9. Access Control

Access is governed via Access Manager and the shared-device security model.

- **Nurse authentication** is required before any access on either tablet surface; anonymous or unattended display is explicitly prohibited
- **Auth methods supported:** Badge tap, PIN, QR fallback — configurable per device policy by Admin
- **User switching** must be fast and secure; the outgoing nurse's session must be cleanly terminated before the incoming nurse's session begins
- **Automatic logout** is triggered by two independent conditions:
- Inactivity timeout, as configured in device policy (Admin Control Plane)
- Rota end time — when the authenticated nurse's shift end time is reached as supplied by Rota Manager, the session must be terminated automatically regardless of activity state
- **Role-scoped access:** nurses see only appointments and tasks relevant to their rota assignment; Admin users may configure which work packages surface on which tablet surface
- MFA requirements for shared devices are governed by Access Manager device policy; this module must honour whatever policy Access Manager enforces and must not bypass it.

10. Integration Summary

- **Appointment Manager** — inbound today-only, rota-context-filtered appointment feed; read/sync
- **Rota Manager** — inbound day-of nurse assignment, shift windows, and break segments as a read-only feed; used to filter both surfaces by rota-assigned surgery and nurse context and to supply rota end-time for session termination; read/sync
- **Task Manager** — inbound decon work packages and lifecycle state; outbound task completion events; async
- **Digital Forms** — inbound mandatory form gate status per appointment (re-queried at Finish & Send initiation); outbound signature capture delegation; sync
- **Aftercare Manager** — outbound aftercare delivery trigger on Finish & Send; event
- **PMS** — inbound appointment record (system of record); outbound appointment progress synchronisation; write/sync
- **Access Manager** — RBAC, shared-device session state machine, and session policy enforcement; read
- **Audit & Compliance** — outbound immutable event log for all governed actions; event
- **Communication Hub** — *(no direct integration captured in original — needs definition)*
- **Lab Manager** — inbound `LabRequired` and `LabCaseReference` per appointment (read-only); inbound unreceipted lab case status for pre-session readiness signalling when module is enabled; enriched lab case status in future; read/sync
- **Inventory & Compliance Manager** — instrument/consumable context overlays and compliance flags when module is enabled (future)

11. Explicit Non-Goals

- **Instrument databases or kit lists** — would be owned by Inventory & Compliance Manager if introduced
- **Treatment-code-to-kit mapping or AI kit mapping** — explicitly excluded from MVP; would be owned by Inventory & Compliance Manager

- **Lab workflow automation** — explicitly excluded from MVP; would be owned by Lab Manager; only lab-required awareness signals are in scope
- **Emergency workflow logic** — explicitly excluded from MVP scope; no module ownership assigned at this time
- **Anonymous or unattended display** — prohibited by design; this module must always require a named, authenticated session
- **Appointment booking rules or diary logic** — owned by Appointment Manager
- **Staffing and coverage planning** — owned by Rota Manager

12. Versioning & Governance

This specification is owned by: Clinical Operations module owner.

Changes to this spec require:

- Review by the MVP module owner
- Impact analysis across all declared related modules (see /propose)
- Preservation of the following non-negotiable design principles:
- Separation of concerns between Decon Wall Tablet and Surgery Tablet surfaces
- Mandatory tooth-level context on both surfaces
- Auditability and named accountability on shared devices
- MVP discipline — explicit exclusions remain excluded unless formally introduced via a governed scope change
- Version bump (patch / minor / major) as appropriate to the nature of the change

13. Build Contract (Engineering & QA)

13.1 Canonical Data Model

```
AppointmentDayRow (read model)
 AppointmentId           UUID
 StartTime               TIMESTAMPTZ
 SurgeryId               UUID
 SurgeryName             TEXT
 ClinicianId             UUID
 ClinicianName           TEXT
 AppointmentTypeId       UUID
 AppointmentTypeName     TEXT
 ToothNumbers            TEXT[]        -- mandatory to surface where available
 LabRequired             BOOLEAN       -- read-only; sourced from Appointment Manager
                                       -- feed (MVP) or Lab Manager (when enabled);
                                       -- must not appear as a write target
 LabCaseReference        TEXT          -- nullable; read-only; same sourcing rules
                                       -- as LabRequired
 Notes                   TEXT          -- nullable

TrayReadiness (write model; Surgery Tablet only)
 AppointmentId           UUID
```

```
 TrayReady               BOOLEAN
 TrayReadyTimestamp      TIMESTAMPTZ
 TrayReadyByUserId       UUID

WorkPackageTaskRow (read/write)
 TaskId                  UUID
 WorkPackageId           UUID
 TaskName                TEXT
 DueTime                 TIMESTAMPTZ
 Status                  TEXT          -- Active | InProgress | Blocked |
                                       -- Completed | Cancelled
 CompletedTimestamp      TIMESTAMPTZ   -- nullable
 CompletedByUserId       UUID          -- nullable

SharedDeviceSession
 DeviceId                UUID
 UserId                  UUID
 AuthMethod              TEXT          -- Badge | PIN | QR
 LoginTimestamp          TIMESTAMPTZ
 LogoutTimestamp         TIMESTAMPTZ   -- nullable; set on explicit logout
 TimeoutTimestamp        TIMESTAMPTZ   -- nullable; set on auto-termination
 -- NOTE: this projection must conform to Access Manager's canonical session
 -- state machine; Access Manager is the authoritative enforcement layer.

AuditLog (immutable)
 EventId                 UUID PRIMARY KEY
 EventType               TEXT
 ActorUserId             UUID
 DeviceId                UUID
 RelatedObjectId         UUID          -- nullable; appointment, task, session ref
 OccurredAt              TIMESTAMPTZ
 Payload                 JSONB         -- event-specific detail; immutable after write
```

13.2 Core Behaviour Rules

Numbered testable behavioural rules that engineering must implement and QA must verify:

1. No authenticated session → no access on either tablet surface; anonymous or unattended display is prohibited.
2. The Decon Wall Tablet is an awareness and compliance surface only; it must not expose per-appointment action controls or become a micro-task execution surface.
3. Tray Ready confirmation is available on the Surgery Tablet only and must record nurse identity (UserId) and timestamp at the moment of confirmation.
4. Both tablet surfaces display today-only appointments filtered by the authenticated nurse's rota assignment; no appointments from other dates or other nurses' rota contexts are surfaced.
5. Tooth numbers must be surfaced on both tablet surfaces where the data is available in the appointment record; this is required context for safe preparation.
6. Decon compliance tasks must display due time, current lifecycle status, completed-by attribution (where completed), and a distinct visual overdue indicator when the due time has passed and the task is not yet completed.
7. Blocked tasks must receive a distinct visual treatment on both surfaces; nurses must not be left silently waiting on a task that cannot complete.

8. Each appointment shown must be backed by a valid Rota Entry from Rota Manager; slots inferred from historical patterns or schedule history must not be surfaced.

9. Break and non-working segments from the Rota Manager feed must be excluded from the appointment view and must never appear as available or actionable slots on either surface.

10. Shared device sessions are automatically terminated by two independent triggers: (a) inactivity timeout as configured in Admin device policy, and (b) rota end time as supplied by Rota Manager — whichever occurs first.

11. Mandatory forms (as defined by Digital Forms) must visibly block in-chair workflow progression on the Surgery Tablet until the form is satisfied; the block must be visible to the nurse prior to and during the session.

12. Finish & Send is a hard gate: it MUST be unavailable while any mandatory form for the appointment is unsigned or incomplete as reported by Digital Forms. The module MUST re-query or receive a push update from Digital Forms at the point the nurse initiates Finish & Send. No user role may bypass this gate.

13. All signature capture on the Surgery Tablet must delegate to and satisfy Digital Forms' governed signing rules, including time-stamped and version-locked capture; no informal or lightweight substitute signature path is permitted.

14. When Lab Manager is enabled, unreceipted lab cases for today's sessions must be surfaced as a distinct pre-session readiness signal, separate from the general lab case reference overlay on the appointment row.

15. Appointment progression synchronisation to the PMS is triggered by Finish & Send and must not occur via any other code path.

16. On session termination — by any trigger (explicit logout, inactivity timeout, or rota-end-time auto-logout) — all locally cached patient-bound data, appointment data, and session credentials MUST be purged from device storage before the login surface is presented. A new session must not be able to access data from the preceding session.

17. `LabRequired` and `LabCaseReference` fields in AppointmentDayRow are display-only; they must not appear as editable or writable fields in TrayReadiness, WorkPackageTaskRow, or any other write surface exposed by this module.

13.3 Configuration Surfaces

Admin Control Plane (practice-level settings):

- Device authentication methods enabled per device (Badge / PIN / QR)
- Inactivity timeout duration for shared device sessions
- Which work packages surface on the Decon Wall Tablet vs the Surgery Tablet

Access Manager (per-role settings):

- Nurse role access scope — what is visible in nurse mode on each surface

Per-device overrides:

- *(no content captured in original — needs definition)*

13.4 Filtering & Views

Views must support:

- Filtering and grouping by surgery and time order (ascending)
- "Imminent / Next" emphasis as the default day-of ordering — upcoming appointments are prioritised visually

- Highlighting of lab-required appointments
- Distinct visual flags for overdue work packages
- Exclusion of break and non-working segments from the appointment list without surfacing them as gaps or bookable slots

13.5 Module Extension Map

When additional modules are enabled, the following surface expansions apply without breaking the MVP contract:

- **Lab Manager** — lab case reference and status visibility is enriched on appointment rows; a distinct "cases awaiting receipt before sessions" signal is surfaced for lab cases that have not yet reached a Received state where the dependent appointment is scheduled for today
- **Inventory & Compliance Manager** — instrument and consumable context overlays and compliance flags are added to appointment rows and workflow steps

Extensions must be additive only; enabling a future module must not alter the behaviour of MVP-defined surfaces or remove any governed constraint established in this specification.

13.6 Acceptance Criteria

The build of Surgery & Decon Day View is complete when:

- [ ] Decon Wall Tablet displays today's appointment schedule filtered by rota and nurse context
- [ ] Each appointment shown is backed by a valid Rota Entry from Rota Manager; no inferred or pattern-derived slots are surfaced
- [ ] Each appointment row shows all mandatory context fields, including tooth numbers where available
- [ ] Break and non-working segments from Rota Manager are excluded from both tablet views
- [ ] Tray Ready can be confirmed on the Surgery Tablet only, with timestamp and nurse identity recorded
- [ ] Decon compliance tasks surface as work packages with due time, status, completed-by attribution, and overdue highlighting
- [ ] Blocked tasks receive a distinct visual treatment on both surfaces; nurses are not silently left with an unactionable task
- [ ] Shared devices require authentication before access; anonymous usage is impossible
- [ ] Fast user switching is supported; outgoing session is cleanly terminated before incoming session begins
- [ ] Sessions are automatically terminated on both inactivity timeout and rota end time triggers
- [ ] On session termination by any trigger, all locally cached patient-bound data, appointment data, and session credentials are purged before the login surface is presented
- [ ] Mandatory forms block in-chair workflow progression on the Surgery Tablet; blocking state is visible to nurses
- [ ] Finish & Send is unavailable while any mandatory form is unsigned or incomplete; Digital Forms gate state is re-queried or push-updated at the point of initiation; gate cannot be bypassed by any user role
- [ ] Signature capture satisfies Digital Forms' governed signing rules; no informal path is available
- [ ] `LabRequired` and `LabCaseReference` are displayed on both surfaces as read-only fields; they do not appear as write targets in any write surface
- [ ] Appointment data is sourced exclusively from the Appointment Manager today-only, rota-context-filtered feed; no other source is used to construct appointment rows

- [ ] Appointment progression is synchronised to the PMS via Finish & Send
- [ ] When Lab Manager is enabled, unreceipted lab cases for today's sessions are surfaced as a distinct pre-session readiness signal
- [ ] All audit events in §8 are captured with actor identity and timestamp
- [ ] Audit log is immutable and exportable
- [ ] Access control is enforced per §9
- [ ] All non-functional requirements in §14 are met

14. Non-Functional Requirements

- **Performance:** View load on both tablet surfaces must be fast enough for day-of clinical operations; target latency for initial load and for rota-filtered appointment data is *(no target captured in original — needs definition)*. Touch interaction must be responsive with no perceptible lag on single-tap actions (Tray Ready, task completion). Fast login is a mandatory performance requirement; authentication flows must not introduce friction that slows nurse access at the start of a session or during rapid user switching.
- **Reliability:** Both tablet surfaces must degrade gracefully if upstream feeds (Appointment Manager, Rota Manager, Task Manager) are temporarily unavailable — the last successfully loaded state should be displayed with a clear staleness indicator rather than a blank or error screen, so nurses retain operational awareness during brief connectivity interruptions. Shared device session handling must remain stable across rapid user-switching cycles.
- **Scalability:** The module must support multi-site, multi-device deployments. Each device operates within the context of a single practice site; data returned to a device must be scoped to that site's rota, appointments, and work packages only.
- **Security:** No anonymous usage is permitted under any circumstance. All data transmitted between tablet surfaces and back-end services must be encrypted in transit. Data at rest on device (e.g. cached session or appointment data) must be encrypted and must be cleared on session termination. Shared tablet operation must enforce secure session handling and role-scoped access as governed by Access Manager.
- **Privacy:** Patient-bound data (appointment details, tooth numbers, form status) is surfaced only to authenticated, rota-assigned nurses. The module must honour applicable GDPR rights — including the right to erasure for non-audit data — and must apply the data retention policy defined at platform level. Audit log data is exempt from erasure where required for regulatory compliance.
- **Accessibility:** Touch targets must be large and glove-friendly. Navigation depth must be minimal. Both tablet surfaces must meet the platform's baseline accessibility standards for contrast and touch target sizing, given the clinical environment in which they operate.
- **Observability:** The module must export metrics covering session counts (login, switch, timeout events), tray readiness confirmation rates, work package completion rates, and overdue task counts. Structured logs must be emitted for all audit events defined in §8. Distributed tracing must cover the critical path from authentication through appointment data load to first render, to support performance diagnosis in production.

15. Open Questions

1. **Inactivity timeout target value** — the original states that idle timeout is configurable in device policy but does not specify a default or minimum value. What is the platform default and the permitted configuration range?

2. **Performance targets** — no specific latency or throughput targets are captured in the original for view load or authentication. What are the SLA targets for initial load time and touch-response latency that QA should verify?

3. **Decon vs Surgery Tablet work package routing** — the spec states admins can configure which work packages surface on which tablet surface, but the routing rules governing that configuration are not defined. What determines the default assignment, and can individual tasks be overridden?

4. **PMS synchronisation contract** — the spec states appointment progress is synchronised back to the PMS via Finish & Send, but the mechanism (direct write, via Appointment Manager, or via a PMS adapter) is not specified. Which integration path is authoritative?

5. **Communication Hub integration** — the original integration summary does not include Communication Hub, but it is a platform-standard module. Is there a notification or alert surface expected from this module (e.g. overdue task escalation alerts), and if so, does Communication Hub own that transport?

6. **Web portal surface** — §5.1 is not addressed in the original; it is unclear whether any web-portal view of day-view data is planned or out of scope for MVP.

7. **Per-device configuration overrides** — the spec identifies practice-level and role-level configuration but does not define what (if anything) can be overridden at the individual device level. Does this need to be defined before build?

8. **Appointment Manager feed update frequency** — the inbound Appointment Manager contract is declared as read/sync, but the update frequency and push/pull mechanism (polling interval, websocket, or server-sent event) are not yet specified. This must be confirmed before build to ensure the today-only view remains current throughout the clinical day.