Access Manager

Doc type: technical · **Version:** v0.1 · **Status:** published · **Module slug:** access-manager
Exported: 2026-05-15 11:10 UTC · **By:** anonymous

Access Manager – Technical Specification

1. Module Purpose & Scope (Authoritative)

Access Manager is the core identity, authentication, and authorisation layer for the Primoro platform. It controls who can access Primoro, what they can see and do, and when and where that access applies — underpinning every other module. No action in Primoro occurs without passing through it.

It governs:

- User identity and authentication across all user types (staff, patients, locums, external parties)
- Role-Based Access Control (RBAC), including custom role configuration and permission toggles
- Joiner, mover, leaver, and locum workflows; guardian, proxy, and family access control
- Session management and token revocation, including mid-session permission propagation
- Consistent access enforcement across web portal, staff app mode, patient app, and in-practice tablets
- Full audit logging of all access decisions for governance and inspections

It explicitly does not:

- Execute business workflows or business logic (owned by the relevant feature modules)
- Manage scheduling or coverage (owned by Rota Manager)
- Orchestrate messaging (owned by Communication Hub)
- Maintain HR records or provide analytics dashboards (owned by Smart Dashboards)
- Apply clinical decision-making (owned by the PMS)

2. Ownership & Responsibilities

2.1 Access Manager IS Responsible For

- Individual user identity: every person has a named account; no shared, generic, or anonymous logins are permitted, and all actions are permanently attributable
- RBAC enforcement at API, UI, and document-category level across every delivery surface
- Custom role configuration: renaming roles, creating custom role labels, toggling module access and document-category visibility — all within governed security tiers
- Device-aware and context-aware access control (personal vs. shared device distinction is honoured)
- Joiner, mover, and leaver lifecycle workflows including immediate revocation on departure
- Locum and temporary staff access (time-bounded, shift-synced, local-auth only)
- Guardian, proxy, and family access control including teen transition and automatic revocation at 18

- Session management: issuance, idle timeout, role-scope embedding, mid-session propagation, and central token revocation
- Audit logging for all access decisions and identity lifecycle events (see §8)
- Gating all data visibility and action authorisation for AI-initiated requests (see §7)
- Emitting access-revocation and session-termination events consumed by downstream modules (Task Manager, Document Hub, Smart Dashboards, Staff App Mode)

2.2 Access Manager IS NOT Responsible For

- Business workflow execution — owned by Task Manager
- Scheduling and shift coverage — owned by Rota Manager
- Messaging orchestration — owned by Communication Hub
- Analytics and reporting surfaces — owned by Smart Dashboards
- Clinical decision-making — owned by the PMS
- HR record management — owned by HR & People Manager; Access Manager consumes HR lifecycle events but does not own the employment record
- Executing the ACP just-in-time support approval workflow — owned by Admin Control Plane; Access Manager enforces the resulting session constraints but does not orchestrate the approval

3. Core Objects (Normative)

3.1 User (Canonical Artefact)

A User is a governed digital identity representing a single named person with access to one or more Primoro surfaces.

Minimum required fields:

- UserId
- UserType (`Staff | Patient | Locum | ExternalParty`)
- CoreRoleType
- CustomRoleId (optional)
- Status (`Active | Suspended | Revoked`)
- CreatedBy (admin actor)
- CreatedAt
- AuditTrail (immutable)

Relationship to HR & People Manager StaffRecord. For staff users, the authoritative employment record resides in HR & People Manager as a `StaffRecord`. Access Manager's `User` object is the governed digital-identity counterpart. Staff lifecycle events — joiners, role changes (movers), and departures (leavers) — originate in HR & People Manager and are propagated inbound to Access Manager, which applies the corresponding User state-machine transitions. Access Manager MUST NOT create or modify a staff User's employment status independently; it consumes HR lifecycle signals and translates them into access state. The integration is described further in §5.

3.2 Session (Canonical Artefact)

A Session represents a single authenticated interaction context issued to a User on a specific device.

Minimum required fields:

- SessionId
- UserId
- DeviceId
- AuthMethod
- IssuedAt
- ExpiresAt
- RoleScopeId

Delegated-context sessions. When a guardian, proxy, or family member accesses a linked patient's record through the Family Profiles profile switcher, a delegated-context session is established. This session carries an additional `OnBehalfOfPatientId` field and a `DelegationScopeId` referencing the granted permission set. The delegated session is distinct from the actor's own direct session; switching context requires re-validation of the active delegation grant (consent currency check) and is logged as a distinct session-switch event in the audit trail (see §4.5). Switching between own-record and dependant-record contexts does NOT require full re-authentication, but MUST re-validate the delegation grant against the current consent record.

ACP SupportSession alignment. Admin Control Plane defines a `SupportSession` artefact for just-in-time elevated support access. Access Manager is responsible for enforcing the session constraints specified in the ACP's SupportSession record (time-box, scope restriction, mandatory MFA) but does not own the approval workflow or the SupportSession object itself. The ACP instructs Access Manager to issue or terminate a constrained session; Access Manager applies its standard session-lifecycle and revocation rules to that session and logs all events in the audit trail.

3.3 PermissionOverride (Canonical Artefact)

A PermissionOverride records a practice-configured departure from a role's default permissions.

Minimum required fields:

- RoleId
- Module
- Category
- Allowed (bool)

3.4 AuditEvent (Canonical Artefact)

An AuditEvent is an immutable record of a discrete identity or access decision made by Access Manager.

Minimum required fields:

- EventType
- Actor
- Target
- Timestamp

Relationship to Security & Privacy SecurityEvent. Security & Privacy defines a platform-wide `SecurityEvent` canonical artefact as the unified audit record for security-relevant actions. Access Manager's `AuditEvent` is the

module-local representation. Access Manager MUST emit its events in a form compatible with the SecurityEvent schema defined by Security & Privacy (or delegate emission to Security & Privacy's ingestion pipeline) so that no deduplication or reconciliation is required. Where a revocation, deletion, or access-change action is marked irreversible by the security-privacy module's rules, Access Manager MUST surface the corresponding irreversibility signal in the UX at the point of action (e.g. leaver revocation, account deletion). The two objects MUST NOT diverge in their coverage of access-lifecycle events; Security & Privacy's schema is authoritative for the platform-level record structure.

3.5 User State Machine (Authoritative)

States:

- `Active` — user has valid access; sessions may be issued
- `Suspended` — access temporarily blocked; existing sessions revoked; record preserved
- `Revoked` — access permanently removed; all sessions force-terminated; historical audit preserved

Rules:

- State transitions are auditable and time-stamped
- A `Revoked` user MUST NOT be returned to `Active` without a new provisioning action, which is itself audited
- Leaver revocation MUST be immediate across all devices; no manual clean-up step is permitted
- Suspension and revocation both trigger immediate forced logout across all active sessions

4. Identity, Authentication & Access Control

4.1 Staff Authentication (Authoritative)

Supported methods:

- SSO via Microsoft Entra ID (Azure AD)
- SSO via Google Workspace
- Local Primoro login (for locums and external staff)
- Optional MFA and biometrics

Hybrid environments combining SSO and local authentication are supported and expected.

Admin Control Plane (ACP) elevated profile. Identities operating the Admin Control Plane are subject to a distinct, elevated authentication contract:

- MFA is mandatory and cannot be waived by practice configuration
- Session lifetimes are shorter than standard staff sessions, configurable within a platform-defined maximum
- Service-to-service automation actions MUST use short-lived, scoped service tokens; human admin credentials MUST NOT be used for automated processes
- All ACP authentication events are logged as a distinct event type in the audit trail

This elevated profile applies to any identity granted ACP-level privileges, regardless of whether the user also holds a standard staff role.

Staff App Mode authentication and session contract. Staff App Mode authenticates through Access Manager using the same supported methods (SSO, MFA, local credentials for locums). Server-side role or access changes

MUST apply immediately to active Staff App Mode sessions without requiring re-login, within the platform-defined propagation window. Terminated sessions MUST NOT be resumable from the client; Staff App Mode consumes the real-time access-revocation signal from Access Manager to enforce this. The staff/patient surface separation enforced by Staff App Mode ("staff/patient mode integrity") is governed by Access Manager's RBAC; a user authenticated in a staff role MUST NOT gain access to patient-surface data through Staff App Mode beyond what their role permits. Role-scoped clarity (each staff role sees only the surfaces, widgets, and records their role permits) is an enforcement contract owned by Access Manager and honoured by Staff App Mode.

4.2 Patient Authentication (Authoritative)

- Passwordless login by default (OTP)
- Optional password combined with biometrics
- Family and guardian accounts supported
- Proxy access for delegated adult care

Patients MUST NOT authenticate through staff identity systems.

4.3 Session Management (Authoritative)

Every session is issued with the user's current role scope embedded. The session token carries a `RoleScopeId` reflecting the active role at issuance. Permission checks during a session are evaluated against the role scope in the token, not re-derived from the user record on each request.

Mid-session permission propagation. When a role assignment or permission override changes for a user with active sessions, Access Manager MUST propagate that change immediately to all active sessions — not solely on next login. This includes role changes that expand or restrict module access, permission toggle changes, and site or group context changes. Consuming surfaces MUST honour an updated role scope signal within a platform-defined propagation window without requiring the user to log out and back in. Full revocation (leaver or suspension) continues to trigger immediate forced logout across all devices.

Real-time revocation signal for downstream modules. When a session is force-terminated or a permission is revoked mid-session, Access Manager MUST emit a structured revocation event that downstream modules can consume synchronously. Document Hub relies on this signal to terminate active document-viewing sessions immediately when access is withdrawn; Staff App Mode relies on it to enforce non-resumable session termination. Access Manager MUST guarantee that the revocation event is emitted atomically with the permission state change — there MUST be no window during which the permission record is updated but the revocation signal has not yet been dispatched. The latency SLA for revocation event delivery is subject to the platform-defined propagation window (see §15, Open Question 1), but revocation of a leaver or suspended user is treated as an immediate hard requirement with no grace period.

Locum access-expiry signalling. When a locum's access window expires (automatically or via manual override), Access Manager MUST emit a structured access-window-expired event. Smart Dashboards consumes this signal to enforce that the locum is redirected to the login screen if a session is active at the time of expiry. This signal follows the same revocation event contract as other session-termination events; no separate mechanism is required.

Additional session rules:

- Idle timeout is enforced
- Central token revocation is available
- Device-level trust is configurable

4.4 RBAC and Role Architecture (Authoritative)

Primoro enforces role-first access using five core role types:

- Front-of-House (FOH)
- Treatment Coordinator (TCO)
- Practitioner
- Dental Nurse
- Manager

Each core role has defined default permissions, a dashboard mapping, and module visibility rules. Permissions are enforced consistently at API, UI, and document-category level.

Document-level enforcement context. Enforcement at document-category level respects two additional dimensions beyond role: patient relationship (whether the acting user has a current clinical or administrative relationship with the patient in question) and site/group context (whether the user's active session is scoped to the site or group that owns the document). Unauthorised documents MUST NOT appear in lists or search results — omission is part of the enforcement contract, not merely a UI preference. These context dimensions are provided to Access Manager by the requesting module and are evaluated as part of every permission decision.

Module-specific operational roles. Roles such as Lab Coordinator, Lab User (External), Inventory Manager, Compliance Manager, and Compliance Officer are represented as custom roles mapped to the closest appropriate core role type (typically Manager or Practitioner). Module owners MUST declare the required core-role mapping at configuration time. All customisation actions are audited.

Module-specific permission scopes. The following module-level permission scopes are governed by Access Manager's RBAC layer. Each maps to the core role types permitted to hold that permission by default; practices may further restrict (but not elevate beyond security-tier limits) via custom role configuration.

> **Campaign Manager** — `campaign:create`, `campaign:read`, `campaign:update`, `campaign:activate`, `campaign:pause`, `campaign:cancel`, `campaign:delete`, `campaign:approve`. Authoring permissions (create, update) are available to Manager and TCO by default; approval permission is restricted to Manager. Campaign authoring or approval roles are assigned via Access Manager and referenced by Campaign Manager at runtime.
>
> **Referral Manager** — `referral:create`, `referral:read`, `referral:assign-owner`, `referral:trigger-transition`, `referral:escalate`, `referral:triage-inbound`. Only users with an authorised role (Practitioner, TCO, or Manager by default) may trigger state transitions or own referral records. Inbound triage is restricted to Manager and TCO by default. Role ownership for referrals is declared at the referral record level and enforced by Access Manager.
>
> **AI Quality Monitor** — `quality-monitor:review-evidence`, `quality-monitor:access-clips`, `quality-monitor:configure-zones`, `quality-monitor:administer-zones`. Evidence-clip access is restricted to Quality Monitor Reviewer (a custom role mapped to Manager or Practitioner). Zone configuration and administration are restricted to Zone Administrator (a custom role mapped to Manager). Access Manager enforces these permission scopes at the API level.
>
> **Aftercare Manager** — `aftercare:trigger-transition`, `aftercare:mark-resolved`, `aftercare:escalate`. Only authorised staff roles (Practitioner and Dental Nurse by default for clinical transitions; Manager for escalation and resolution) may manually trigger transitions from Prepared to Delivered or mark a record Resolved. Role definitions are declared here and enforced at the Aftercare Manager API boundary via Access Manager.

Loyalty Insights — `loyalty:view-cohort-insights`, `loyalty:view-practitioner-linked-cohorts`. Practitioner-linked cohort insight is restricted to authorised managerial roles (Manager by default). Practitioners may view their own cohort summary but MUST NOT access other practitioners' linked cohort data. All access to cohort insight is audit-logged.

AI Meeting Notes — `meeting-notes:enrol-voice-profile`, `meeting-notes:view-transcript`, `meeting-notes:view-summary`, `meeting-notes:delete-transcript`. Voice profile enrolment is restricted to the individual staff member enrolling their own profile (self-enrolment only) and to Manager for administrative revocation. Transcript and summary access is restricted by role and patient-relationship context in the same manner as clinical documents. Voice profile data is treated as biometric-adjacent personal data; enrolment and deletion events are audit-logged.

Performance Dashboards and Smart Dashboards — role-bound dashboard views align directly to the five core role types (FOH, TCO, Practitioner, Dental Nurse, Manager). The Manager/Owner view and the Group/Multi-Site view are scoped by the user's site/group context embedded in the session. Access Manager's role definitions are the authoritative source for dashboard role-binding; no dashboard module may define role boundaries independently. Locum and temporary staff accounts MUST NOT be issued sessions with Manager-level dashboard scope.

Financial Insights — `financial:approve-statement`, `financial:verify-statement`, `financial:distribute-statement`, `financial:view-reports`. Approval and verification permissions are restricted to Manager by default. All permission changes and revocations affecting financial approval authority are audit-logged, enabling Financial Insights to validate approval authority at the time of any given action.

Aiden (AI Assistant) role-based guidance filtering. Aiden is a consuming module subject to Access Manager's RBAC at all times. Access Manager gates Aiden's context resolution and action recommendations per the current session's role scope: Aiden MUST NOT surface records, suggest actions, or resolve context that the session's role scope does not permit. This is enforced via the same permission-decision mechanism described in §7. Practice configuration MUST NOT grant Aiden capabilities that exceed the role permissions of the authenticated user.

External Party access tier. External referrers and external lab users — parties who are neither staff, patients, nor locums but require scoped, auditable access — are provisioned as an External Party access tier. External Party accounts are:

- scoped strictly to the records and actions assigned to them
- unable to access internal administrative surfaces
- subject to the same audit, session, and revocation controls as staff
- authenticated via local Primoro login (not SSO)
- time-bounded or referral/case-bounded where appropriate

Custom roles (controlled flexibility). Practices may rename roles, create custom role labels, toggle module access, and toggle document-category visibility. Every custom role maps to a core role type. Practices cannot bypass fundamental security tiers regardless of how roles are named or customised. All customisation actions are audited.

4.5 Family Profiles, Guardian, and Delegated-Access Session Management (Authoritative)

Guardian, proxy, and family access is described in §2.1 at a high level. This section defines the session and authentication contract.

Profile-switcher session transitions. The Family Profiles module provides a persistent profile switcher enabling a guardian or proxy to switch between their own patient record and linked dependant records within the patient app. Access Manager governs this transition as follows:

- The actor's primary session remains active throughout; no full re-authentication is required to switch context.
- On each context switch to a dependant's record, Access Manager MUST re-validate the active delegation grant: it checks that the consent record for the `(actor, dependant)` pair is current, that the requested action falls within the granted permission set, and that the dependant's record has not been age-transitioned or revoked since the last validation.
- If re-validation fails (consent withdrawn, age transition passed, scope mismatch), the context switch MUST be denied and the actor MUST be returned to their own-record context.
- Delegated sessions carry `OnBehalfOfPatientId` and `DelegationScopeId` in addition to the standard session fields (see §3.2).
- Each context switch is logged as a `DelegatedContextSwitch` audit event with actor, target patient, delegation scope, validation outcome, and timestamp.
- Delegated sessions are subject to the same idle timeout, revocation, and mid-session propagation rules as direct sessions.

Teen transition and automatic revocation. When a dependant patient reaches the age threshold for guardian access revocation (age 18 by default, or the platform-configured threshold), Access Manager automatically revokes all delegation grants for that patient, terminates any active delegated sessions, and logs the revocation event. The guardian is notified via Communication Hub. No manual intervention is required.

Audit distinction. Audit events generated during delegated-context sessions MUST record both the actor's UserId and the `OnBehalfOfPatientId` so that the audit trail clearly distinguishes delegated access from the dependant's own direct access.

5. Joiners, Movers & Leavers

5.1 Joiners

- Rapid onboarding with role-assigned access
- Immediately available across all delivery surfaces

Inbound from HR & People Manager. Staff joiner records originate in HR & People Manager as a `StaffRecord` creation event. Access Manager consumes this event and provisions the corresponding `User` object with the specified role. The provisioning action is audited with the HR event reference. Access Manager MUST NOT create a staff User without a corresponding HR record reference unless the user type is non-staff (Patient, Locum, ExternalParty).

5.2 Movers

- Role changes update access instantly
- No duplicate accounts are created

Inbound from HR & People Manager. Role changes and site/group reassignments originate in HR & People Manager as `StaffRecord` update events. Access Manager consumes these events and applies the corresponding User role-update and mid-session permission propagation immediately. The update is audited with the HR event reference.

5.3 Leavers

- One-click access removal
- Immediate revocation across all devices
- Historical audit record preserved

No access removal relies on manual clean-up.

Inbound from HR & People Manager. Staff departure is signalled from HR & People Manager as a `StaffRecord` leaver event. Access Manager consumes this event and transitions the User to `Revoked` immediately, force-terminating all active sessions.

Leaver event schema for downstream consumers. When a User transitions to `Revoked` via the leaver workflow, Access Manager MUST emit a structured `UserRevoked` event with the following minimum fields:

- `UserId`
- `RevokedAt` (timestamp)
- `RevokedBy` (actor)
- `Reason` (`Leaver | Suspension | ManualRevocation`)
- `ActiveSessionsTerminated` (count)
- `HREventReference` (nullable; present for HR-originated leavers)

Task Manager consumes this event to revert in-flight task ownership to role queues before the user loses access. The event MUST be emitted atomically with the session force-termination; Task Manager MUST receive the event no later than the point at which the sessions are terminated so that no task ownership gap exists.

6. Locum & Temporary Staff Access

Locum access is created via Rota Manager, role-scoped, time-bounded, and synced to scheduled shifts. Locums are excluded from full administrative surfaces by default.

The module MUST:

- Restrict locum authentication to local Primoro login (not SSO)
- Activate access only around scheduled work periods
- Expire access automatically after inactivity
- Audit any manual override of expiry
- Emit a structured `LocumAccessExpired` event when access expires (automatically or via override), consumed by Smart Dashboards and other surfaces to enforce immediate session termination

The module MAY:

- Allow a practice administrator to extend locum access manually, subject to audit

The module MUST NOT:

- Grant locums access to ACP-level surfaces
- Allow locum credentials to persist beyond their defined expiry without an audited override
- Issue locum sessions with Manager-level dashboard scope

7. AI Boundaries (Non-Negotiable)

Access Manager is the enforcement point for all AI-initiated data access decisions. It actively gates all data visibility and action authorisation for requests made by AI Assistant (Aiden), enforcing that no cross-role data leakage occurs, no patient data is surfaced without verified context, and no staff action is taken without explicit authorisation.

AI MAY:

- Receive permission decisions from Access Manager that it must honour in determining what data to surface or actions to propose
- Surface to staff only the records and actions that Access Manager has authorised for the current session context

AI MAY NOT:

- Bypass Access Manager's RBAC or session-scope checks
- Access patient data without a verified session context and explicit authorisation from Access Manager
- Trigger actions that would circumvent role restrictions
- Make access-policy decisions autonomously; all access decisions are owned by Access Manager
- Replace or shortcut audit logging of AI-initiated access requests

RBAC enforcement decisions for AI-initiated requests are logged by Access Manager as a distinct event class within the audit trail, satisfying the requirement that audit ownership resides with the underlying governing module.

8. Audit & Compliance

8.1 Audit Logging (Mandatory)

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

- Login and logout (all user types)
- Failed authentication attempts
- MFA challenges and outcomes
- ACP authentication and session events (as a distinct event type)
- ACP SupportSession issuance and termination events (as a distinct event type, aligned with the ACP SupportSession artefact)
- Role assignment changes
- Permission toggle changes
- Custom role creation and modification
- Locum access activation and expiry
- Manual override of locum expiry
- Guardian and proxy access changes (grant, scope change, revocation)
- Delegated context-switch events (`DelegatedContextSwitch`), including validation outcome and on-behalf-of patient reference
- Teen-transition auto-revocation events

- Token revocation events
- Session force-termination events
- `UserRevoked` leaver events (including `HREventReference` where applicable)
- Voice profile enrolment, update, and deletion events (`meeting-notes:enrol-voice-profile`)
- Permission overrides and revocations affecting financial approval authority (enabling Financial Insights to validate approval authority at time of action)
- RBAC enforcement decisions for dashboard access and role-based visibility (owned by Access Manager as the governing RBAC layer, satisfying Smart Dashboards' audit-ownership requirement)
- RBAC enforcement decisions for AI-initiated data access requests

Audit logs MUST be immutable and exportable for inspection. Historical records MUST NOT be re-attributed following any access change. Where an event is marked irreversible (leaver revocation, account deletion), the audit entry MUST record this irreversibility flag in alignment with the Security & Privacy SecurityEvent schema. All audit events MUST be emitted in a form compatible with the platform-wide SecurityEvent schema (see §3.4).

8.2 Compliance Posture

Access Manager's audit trail is designed to support regulatory inspection and clinical governance requirements. All identity lifecycle events and access decisions are retained in the immutable log regardless of the user's current status.

9. Access Control

The following operations and their permitted actors apply within Access Manager itself:

- **Provision / create user** — Practice Administrator, ACP-level identity
- **Read user record and access history** — Practice Administrator; Managers (within their site scope); the user themselves (own record only)
- **Modify role assignment or permission override** — Practice Administrator, ACP-level identity
- **Suspend user** — Practice Administrator, ACP-level identity
- **Revoke user (leaver)** — Practice Administrator, ACP-level identity
- **Extend or override locum expiry** — Practice Administrator (audited)
- **Configure SSO, MFA rules, session timeouts** — ACP-level identity only
- **Enrol or delete own voice profile (AI Meeting Notes)** — the individual staff member (self only); Manager for administrative deletion
- **Administer delegation grants (guardian/proxy)** — Practice Administrator; the patient themselves (where capacity permits); guardian (within granted scope)

MFA is mandatory for all ACP-level identities and cannot be waived. MFA is optional but configurable for standard staff. Patients authenticate separately and are never subject to staff MFA policies.

10. Integration Summary

- **Rota Manager** — inbound; locum access records are created from scheduled shifts defined in Rota Manager

- **Task Manager** — outbound; joiner/mover/leaver workflow steps may generate tasks for human follow-up; Task Manager also consumes the `UserRevoked` event to revert in-flight task ownership to role queues
- **Communication Hub** — outbound; access lifecycle events (e.g. new user provisioned, leaver confirmed, teen-transition guardian revocation) may trigger notifications
- **Smart Dashboards** — RBAC enforcement; Access Manager governs dashboard and widget visibility by role and owns the audit events for those decisions; Smart Dashboards consumes `LocumAccessExpired` and session-revocation events to enforce immediate redirect on expiry
- **Document Hub** — RBAC enforcement; document-category visibility is gated by Access Manager using role, patient-relationship, and site/group context; Document Hub consumes real-time revocation events to terminate active viewing sessions immediately
- **Staff App Mode** — delivery surface; must honour mid-session role scope updates within the platform-defined propagation window; consumes real-time revocation signal for non-resumable session termination; staff/patient surface separation and role-scoped clarity are enforced by Access Manager
- **Patient App** — delivery surface; patient authentication is governed by Access Manager; family profile-switcher context transitions are governed by Access Manager's delegated-session contract
- **In-Practice Tablets** — delivery surface; device-context (shared vs. personal) is honoured by Access Manager
- **Admin Control Plane** — governed surface; ACP identities are subject to Access Manager's elevated authentication profile; Access Manager enforces ACP SupportSession constraints but does not own the approval workflow
- **AI Assistant (Aiden)** — enforcement point; Access Manager gates all data visibility and action authorisation for AI-initiated requests; Aiden's context resolution and action recommendations are filtered by the session's role scope
- **HR & People Manager** — inbound; StaffRecord joiner, mover, and leaver events originate in HR & People Manager and are consumed by Access Manager to drive User lifecycle transitions
- **Campaign Manager** — RBAC enforcement; campaign authoring and approval roles are assigned via Access Manager and enforced at runtime
- **Referral Manager** — RBAC enforcement; referral state-transition and ownership-assignment permissions are governed by Access Manager
- **AI Quality Monitor** — RBAC enforcement; evidence-clip access and zone configuration permissions are governed by Access Manager
- **Aftercare Manager** — RBAC enforcement; aftercare state-transition and resolution permissions are governed by Access Manager
- **Loyalty Insights** — RBAC enforcement; practitioner-linked cohort insight access is restricted to authorised managerial roles by Access Manager
- **AI Meeting Notes** — RBAC enforcement and identity; voice profile enrolment is tied to staff identity in Access Manager; transcript and summary access is governed by role and patient-relationship context
- **Performance Dashboards** — RBAC enforcement; role-bound dashboard views are governed by Access Manager's core role definitions
- **Financial Insights** — RBAC enforcement; financial approval and verification permissions are governed by Access Manager; permission changes are audit-logged to support approval-authority validation

11. Explicit Non-Goals

- Executing business workflows — no current module replaces this; it is an inherent non-goal of an access-control layer
- Replacing enterprise IAM platforms — Access Manager integrates with Microsoft Entra ID and Google Workspace but does not replace them
- Managing HR records — explicitly out of scope; owned by HR & People Manager
- Providing analytics dashboards — owned by Smart Dashboards
- Applying policy selectively or allowing security-tier bypass — prohibited regardless of custom role configuration
- Owning the ACP just-in-time support approval workflow — owned by Admin Control Plane; Access Manager enforces the resulting constraints only

12. Versioning & Governance

This specification is owned by: the Access Manager module owner.

Changes to this spec require:

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

All future changes must preserve: individual attribution, role-first access, immediate revocation, platform-wide consistency, and RBAC as a non-negotiable foundation.

13. Build Contract (Engineering & QA)

13.1 Canonical Data Model

```
User (
 UserId          UUID PRIMARY KEY,
 UserType        ENUM('Staff','Patient','Locum','ExternalParty'),
 CoreRoleType    ENUM('FOH','TCO','Practitioner','DentalNurse','Manager'),
 CustomRoleId    UUID NULL,
 Status          ENUM('Active','Suspended','Revoked'),
 CreatedBy       UUID NOT NULL,
 CreatedAt       TIMESTAMPTZ NOT NULL,
 HRRecordRef     UUID NULL  -- references HR & People Manager StaffRecord; required for UserType='Sta
)

Session (
 SessionId           UUID PRIMARY KEY,
 UserId              UUID NOT NULL REFERENCES User(UserId),
 DeviceId            UUID NOT NULL,
 AuthMethod          TEXT NOT NULL,
 IssuedAt            TIMESTAMPTZ NOT NULL,
 ExpiresAt           TIMESTAMPTZ NOT NULL,
 RoleScopeId         UUID NOT NULL,
 OnBehalfOfPatientId UUID NULL,  -- present for delegated-context sessions only
 DelegationScopeId   UUID NULL   -- present for delegated-context sessions only
```

```
)

PermissionOverride (
 OverrideId      UUID PRIMARY KEY,
 RoleId          UUID NOT NULL,
 Module          TEXT NOT NULL,
 Category        TEXT NOT NULL,
 Allowed         BOOLEAN NOT NULL
)

AuditEvent (
 EventId         UUID PRIMARY KEY,
 EventType       TEXT NOT NULL,
 Actor           UUID NOT NULL,
 Target          UUID NULL,
 OnBehalfOf      UUID NULL,  -- populated for delegated-context events
 Timestamp       TIMESTAMPTZ NOT NULL,
 Irreversible    BOOLEAN NOT NULL DEFAULT FALSE,
 SecurityEventRef UUID NULL  -- reference to platform-wide SecurityEvent record
)

UserRevoked (  -- outbound integration event; not a persisted table
 UserId                  UUID NOT NULL,
 RevokedAt               TIMESTAMPTZ NOT NULL,
 RevokedBy               UUID NOT NULL,
 Reason                  ENUM('Leaver','Suspension','ManualRevocation'),
 ActiveSessionsTerminated INTEGER NOT NULL,
 HREventReference        UUID NULL
)
```

13.2 Core Behaviour Rules

1. No shared, generic, or anonymous accounts may exist; every user account maps to a single named individual.
2. Every access decision and identity lifecycle action is attributable to a named actor and logged immutably.
3. Access changes — including role reassignments and permission toggle changes — apply immediately to all active sessions without requiring re-authentication; the propagation window is platform-defined.
4. Locum access is time-bounded and synced to scheduled shifts; automatic expiry MUST occur without manual intervention.
5. Guardian and proxy access requires explicit patient consent, is scoped to granted actions, and is fully auditable.
6. All RBAC decisions — including document-category visibility — are evaluated against role, patient-relationship context, and site/group context provided by the requesting module.
7. Unauthorised records MUST NOT appear in lists or search results; omission is an enforcement requirement.
8. Session tokens carry a `RoleScopeId` at issuance; permission checks are evaluated against the token scope.
9. When a role or permission changes mid-session, Access Manager MUST propagate the updated scope to all active sessions within the platform-defined propagation window.
10. Full revocation (leaver or suspension) triggers immediate forced logout across all devices; the `UserRevoked` event MUST be emitted atomically with session termination.

11. ACP-level identities MUST use mandatory MFA and shorter session lifetimes; this cannot be waived by practice configuration.

12. External Party accounts are scoped strictly to assigned records and actions, cannot access internal administrative surfaces, and are subject to the same audit and revocation controls as staff.

13. All RBAC enforcement decisions for AI-initiated requests are gated and logged by Access Manager.

14. Historical audit records are never re-attributed following any access change, suspension, or revocation.

15. Delegated-context sessions (guardian/proxy/family) carry `OnBehalfOfPatientId` and `DelegationScopeId`; delegation grants are re-validated on every context switch.

16. Staff User objects MUST reference a `HRRecordRef` linking to the authoritative HR & People Manager StaffRecord; staff lifecycle events originate in HR & People Manager and cascade inbound to Access Manager.

17. Revocation events for leaver and suspension actions MUST include an `Irreversible` flag and MUST surface a corresponding irreversibility warning in the UX at the point of action.

18. All audit events are emitted in a form compatible with the platform-wide SecurityEvent schema defined by Security & Privacy; the two MUST NOT diverge in coverage of access-lifecycle events.

19. Voice profile enrolment and deletion are restricted by identity and role; enrolment is self-only for the individual staff member; administrative deletion is restricted to Manager.

13.3 Configuration Surfaces

Practice-level settings (Admin Control Plane):

- SSO provider configuration (Microsoft Entra ID, Google Workspace)
- MFA rules (mandatory for ACP; optional for standard staff)
- Role mappings and custom role labels
- Custom permission toggles per module and document category
- Session timeout values (within platform-defined maxima per identity tier)
- Locum expiry windows
- External Party access scope and expiry
- Delegation grant configuration (guardian/proxy scope and expiry)
- Module-specific permission scope assignments (Campaign Manager, Referral Manager, AI Quality Monitor, Aftercare Manager, Loyalty Insights, AI Meeting Notes, Financial Insights)

Per-user preferences are limited to authentication method selection (where the practice permits optionality), personal device trust settings, and own voice profile enrolment (AI Meeting Notes).

13.4 Filtering & Views

Administrators can filter users and access events by:

- Role (core type and custom label)
- Status (`Active | Suspended | Revoked`)
- Site
- Device
- Access event type
- Delegated-context events (guardian/proxy actions, filtered by on-behalf-of patient)

Audit event views MUST support export in a machine-readable format to support governance inspections.

13.5 Module Extension Map

When enabled, the following extensions integrate with Access Manager without breaking this contract:

- **Governance Reporting** — consumes access audit events for compliance reporting
- **AI Guardian** — consumes access patterns for anomalous access detection (read-only; does not modify access decisions)
- **Group Controls** — enforces multi-tenant site/group separation within Access Manager's RBAC evaluation

13.6 Acceptance Criteria

- [ ] No shared logins exist; every user account maps to a single named individual
- [ ] Access is role-based and enforced at API, UI, and document-category level across all delivery surfaces
- [ ] Document-category enforcement evaluates role, patient-relationship context, and site/group context; unauthorised records are omitted from lists and search
- [ ] Locum access expires automatically without manual intervention; `LocumAccessExpired` event is emitted and consumed by Smart Dashboards
- [ ] Leaver access is revoked instantly across all devices; `UserRevoked` event is emitted atomically with session termination
- [ ] Task Manager receives `UserRevoked` event no later than session termination and correctly reverts in-flight task ownership
- [ ] Audit trail is complete and immutable; all event types in §8 are captured
- [ ] Audit events are compatible with the platform-wide SecurityEvent schema; irreversible events carry the `Irreversible` flag
- [ ] Sessions carry `RoleScopeId`; mid-session permission changes propagate within the platform-defined window
- [ ] ACP-level identities enforce mandatory MFA and shorter session lifetimes; waiver is not possible via practice configuration
- [ ] ACP SupportSession constraints (time-box, scope, MFA) are enforced; issuance and termination events are audit-logged
- [ ] External Party accounts are scoped, time-bounded, and fully audited
- [ ] RBAC enforcement decisions for AI-initiated requests are gated and logged by Access Manager
- [ ] Delegated-context sessions carry `OnBehalfOfPatientId` and `DelegationScopeId`; delegation grants are re-validated on each context switch
- [ ] Teen-transition auto-revocation fires at the configured age threshold without manual intervention
- [ ] Staff User objects reference a `HRRecordRef`; staff lifecycle events propagate from HR & People Manager
- [ ] Module-specific permission scopes (Campaign Manager, Referral Manager, AI Quality Monitor, Aftercare Manager, Loyalty Insights, AI Meeting Notes, Financial Insights, Performance Dashboards) are enforced at the API level
- [ ] Voice profile enrolment is self-only; administrative deletion is restricted to Manager; all events are audit-logged
- [ ] Real-time revocation events are emitted atomically; Document Hub and Staff App Mode enforce immediate session termination on receipt

- [ ] All canonical objects can be created, read, and updated through the API
- [ ] State machine transitions enforce all rules in §3.5
- [ ] All integrations in §10 are wired
- [ ] AI boundaries in §7 are enforced (negative tests pass)
- [ ] All non-functional requirements in §14 are met

14. Non-Functional Requirements

- **Performance:** Authentication and RBAC checks MUST complete with low latency and MUST NOT block or delay UI rendering. Role resolution MUST NOT introduce perceptible lag on page or surface load.
- **Reliability:** Access enforcement MUST remain operational even during partial platform outages. Access Manager MUST degrade gracefully — preferring denial over unguarded permissiveness — when downstream services are unavailable. An availability target appropriate to a foundational security layer (no module bypasses Access Manager) should be defined by the platform engineering team before the MVP build contract is finalised.
- **Scalability:** Access Manager MUST support multi-site and multi-tenant deployments. RBAC evaluation MUST scale linearly with user and session volume without architectural changes.
- **Security:** All credentials and session tokens MUST be encrypted in transit (TLS) and at rest. Secrets and service tokens MUST be managed through a platform-approved secrets management mechanism; human credentials MUST NOT be used for automated processes. Defence against credential reuse is required. Rapid revocation (immediate forced logout on leaver/suspension) is a hard requirement.
- **Privacy:** Access Manager handles personal data (staff identity, patient identity, guardian relationships, voice profile enrolment data) and MUST honour applicable data subject rights including access and erasure requests, subject to the constraint that audit records are immutable. Voice profile data is treated as biometric-adjacent personal data and is subject to the same privacy controls. Data retention periods for user records and audit logs should be defined by the platform governance team before the MVP build contract is finalised.
- **Observability:** Access Manager MUST export metrics covering authentication success/failure rates, session issuance and revocation rates, mid-session propagation latency, RBAC enforcement decision latency, and revocation-event dispatch latency. Structured logs and distributed traces MUST be emitted for all authentication and authorisation paths to support incident investigation.

15. Open Questions

1. **Platform-defined propagation window:** The spec requires mid-session permission changes to propagate within a "platform-defined propagation window" but does not specify the target. What is the acceptable maximum latency for role scope updates to reach active sessions? *(Surfaced from §4.3 and §13.2 Rule 9.)*
2. **ACP session lifetime maximum:** The spec states ACP session lifetimes are "shorter than standard staff sessions, configurable within a platform-defined maximum" but does not specify that maximum. What is the platform-defined upper bound? *(Surfaced from §4.1.)*
3. **Availability target:** No specific availability SLA (e.g. 99.9%) is stated for Access Manager despite it being a foundational layer that every other module depends on. What is the target? *(Surfaced from §14 Reliability.)*
4. **Data retention policy:** Retention periods for user records (post-revocation) and immutable audit logs are not specified. What are the platform-mandated retention windows, and how do they interact with GDPR

erasure rights for staff and patient identities? *(Surfaced from §14 Privacy and §8.)*

5. **Secrets management platform:** The spec requires short-lived scoped service tokens for ACP automation but does not name the secrets management mechanism. Which platform-approved tool manages service credentials? *(Surfaced from §4.1.)*

6. **HR & People Manager event schema:** Access Manager consumes `StaffRecord` lifecycle events from HR & People Manager. The precise event schema (field names, delivery mechanism, ordering guarantees) must be agreed between module owners before the MVP build contract is finalised. *(Surfaced from §5 and §13.1.)*

7. **Delegation grant re-validation latency:** The spec requires re-validation of delegation grants on each Family Profiles context switch. What is the acceptable latency for this check, and how should Access Manager behave if the consent store is temporarily unavailable — deny the switch or allow with a grace period? *(Surfaced from §4.5.)*

8. **Voice profile storage:** AI Meeting Notes voice profile data is governed by Access Manager for enrolment permissions, but the storage and processing of voice data itself is owned by AI Meeting Notes. The boundary between identity (Access Manager) and biometric data (AI Meeting Notes) should be formally agreed before voice enrolment is built. *(Surfaced from §4.4 and §14 Privacy.)*