Family Profiles

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

Family Profiles – Technical Specification

1. Module Purpose & Scope (Authoritative)

Family Profiles enables secure, governed delegation of access between related patients inside Primoro. It allows parents, guardians, and carers to manage dependants' care in a single authenticated session, reduces duplicated accounts and administration, and supports paediatrics, assisted adults, and multi-dependant households — while preserving individual patient records at all times and enforcing explicit consent and auditability throughout.

Family Profiles organises relationships — not medical data. No records are merged and no access is implied by the existence of a relationship.

It governs:

- Defining and managing family and carer relationships between independent patient records
- Delegating authenticated access so one user may act on behalf of linked patients, within explicit permission sets
- Routing communications, forms, aftercare, and appointment actions to the correct responsible party
- Managing age-based transition to patient-managed access
- Maintaining a full, immutable audit trail for all delegated actions

It explicitly does not:

- Manage appointment availability or scheduling rules — owned by **Appointment Manager**
- Own form structure or consent logic — owned by **Digital Forms**
- Handle messaging transport — owned by **Communication Hub**
- Handle payment settlement or plans — owned by **Integrated Payments**
- Store or manage clinical notes or diagnosis — owned by the Practice Management System (PMS / Dentally)

2. Ownership & Responsibilities

2.1 Family Profiles IS Responsible For

- Defining family and carer relationships between patients
- Allowing one authenticated user to act on behalf of linked patients, within an explicit permission set
- Governing who can do what, for whom, via role-based permission sets
- Enabling delegated appointment booking and management (within Appointment Manager rules)
- Enabling delegated Digital Forms completion and consent signing
- Enabling family-aware Aftercare delivery and follow-up routing

- Routing communications to the correct responsible party
- Managing age-based transition to patient-managed access
- Maintaining a full audit trail for all delegated actions, with actor attribution on every event

2.2 Family Profiles IS NOT Responsible For

- Appointment availability or scheduling rules — **Appointment Manager**
- Form structure, consent logic, or form versioning — **Digital Forms**
- Messaging transport and delivery — **Communication Hub**
- Payment settlement, payment plans, or billing logic — **Integrated Payments**
- Clinical notes, diagnoses, or any record held in the PMS — **Dentally (PMS)**
- Task creation workflows beyond triggering — **Task Manager**

3. Core Objects (Normative)

3.1 Family Profile (Canonical Artefact)

A Family Profile is a governed digital artefact representing a structured relationship grouping that enables delegated action between independent patient records.

It:

- Links independent patient records without merging clinical data
- Exists only with explicit consent, recorded at creation
- Can be suspended or revoked at any time
- Is owned by the practice, not by any individual patient or guardian

Minimum required fields:

- FamilyProfileId (immutable)
- FamilyMemberId (per member record)
- PatientId (FK to patient record)
- ActingUserId (FK to authenticated user performing delegation)
- Role (enum: Primary Account Holder | Parent/Guardian | Carer | Dependant)
- PermissionSetId (FK to role-based permission set)
- Status (Active | Pending | Revoked)
- CreatedBy (user/role)
- CreatedTimestamp
- RevokedTimestamp (nullable)
- AuditLog (immutable, append-only)

3.2 Family Profile State Machine (Authoritative)

States:

- **Created** — relationship record initialised; consent pending or invite issued

- **Active** — consent confirmed; delegated access operational
- **Modified** — member list or permissions updated; transition is audited
- **Suspended** — access temporarily disabled without revocation
- **Revoked / Archived** — access permanently removed; record retained for audit

Rules:

- All state transitions are auditable and time-stamped
- A Family Profile cannot return to Active from Revoked/Archived; a new profile must be created
- Revocation takes immediate effect — delegated access is removed at the moment the transition is committed
- Only staff with the appropriate permission set may initiate creation, modification, suspension, or revocation
- Invite-based creation holds the profile in Created/Pending until the guardian redeems the invite and confirms consent

4. Creation, Management & Delegation

4.1 Creation Sources

Staff-initiated linking: Staff verify consent and initiate links via the staff web portal. Links may be activated directly or via a secure one-time invite code.

Invite-based linking: Secure one-time invite codes may be issued by staff. Guardians redeem codes in the patient mobile app to complete linking. Consent confirmation is mandatory before the profile becomes Active.

Dentally-assisted discovery (optional): Dentally "responsible party" data may be used to surface suggested links to staff. No link is auto-created without explicit staff approval. Dentally remains an external reference only and is never written to by this module.

The module MUST:

- Require explicit consent confirmation before any Family Profile becomes Active
- Record the consenting actor, timestamp, and method on the profile record
- Prevent any delegated action until the profile is in Active state

The module MUST NOT:

- Auto-create any relationship link without explicit human approval
- Infer or inherit access between patients outside a created and Active profile

Access Manager Permission Grant Lifecycle

Family Profiles interacts with Access Manager at each stage of the delegation lifecycle. When a Family Profile is created or modified, this module emits the appropriate relationship context to Access Manager so that guardian, proxy, and carer permission grants are created, updated, or revoked in the Access Manager permission model. All such grants MUST be explicitly confirmed — Access Manager requires audited confirmation for access grants, and Family Profiles MUST NOT assume a grant is active until Access Manager acknowledges it.

Where Access Manager surfaces configurable permission toggles for guardian or dependant access (for example, restricting a carer to read-only form access, or limiting a guardian to appointment booking only), those toggles govern the effective permission set enforced by Family Profiles at runtime. Permission set checks are

always resolved server-side via Access Manager on every delegated API request; Family Profiles MUST NOT cache or assume permission state beyond the current request boundary without explicit invalidation on profile modification. Revocation of a Family Profile MUST trigger immediate removal of the corresponding Access Manager grants in the same transaction.

Aftercare Delegation Model

Aftercare Manager supports delivery and escalation to carers and guardians via Family Profiles, with dual attribution on any escalated record: both `PatientId` (the represented patient) and `CarerId` (the acting delegated user) are recorded as distinct fields. Family Profiles MUST supply this dual-attribution context to Aftercare Manager whenever an aftercare interaction is initiated or escalated in a delegated session.

Specifically:

- When a guardian or carer is the active delegated user at the point an aftercare interaction begins or escalates, Family Profiles emits both `PatientId` and `CarerId` as part of the family context event to Aftercare Manager.
- Aftercare Manager uses `CarerId` solely to route delivery and attribute escalation records; it does not grant the carer any additional access to clinical data beyond what their Family Profiles permission set permits.
- Where an aftercare escalation generates a staff task or notification, the represented patient's identity is always the primary attribution; the carer's identity is recorded as the acting party.
- All aftercare interactions initiated or escalated within a delegated session are logged in the Family Profiles audit log with full dual attribution.

4.2 Delegation Rules (Authoritative)

Appointment Management

Delegated users may view, book, cancel, and reschedule appointments for linked dependants, and receive reminders and confirmations on their behalf. Delegated users may also receive Digital Waitlist offers, engage with them, and confirm appointments through the waitlist flow.

When participating in the Digital Waitlist on a dependant's behalf, all Appointment Manager offer-lifecycle rules apply without modification. This includes the broadcast-offer state, the practice-configurable engagement lock window that prevents indefinite reservation, and the resulting Confirmed or Expired states. A delegated user MUST respond to waitlist offers within the same engagement lock window that applies to direct patients; no extended window is granted by virtue of acting on behalf of another.

Digital Forms & Consent

Delegated users may complete forms for dependants and sign as guardian where appropriate. Where the delegated user's permission set includes read access, they may view completed and signed forms for dependants. Where explicitly authorised by their permission set, they may download or securely share signed PDF records.

When a delegated user signs a form on behalf of a dependant, the signing attribution MUST be recorded using Digital Forms' `SigningRole` enum, which defines the following values drawn from this module's relationship model: `Self`, `Parent`, `LegalGuardian`, `AuthorisedCarer`. Family Profiles is the authoritative source for which role value applies — the role is derived from the delegated user's `Role` field on the `family_member` record (Parent/Guardian maps to `Parent` or `LegalGuardian` as appropriate; Carer maps to `AuthorisedCarer`). Digital Forms records both `CarerId` (the `acting_user_id` from the Family Profile) and `SignedByUserId` against every delegated signing event; Family Profiles MUST supply these identifiers in the outbound delegation event so that Digital Forms can enforce that only an active, authorised Family Profile member may sign on a dependant's

behalf.

Only a delegated user whose Family Profile is in Active state and whose permission set includes form-signing authorisation may act as a signing party for a dependant. Family Profiles MUST reject or withhold the signing delegation signal if the profile is in any state other than Active at the moment of signing.

Form records always capture: who signed, on whose behalf, under which form version, and when. Where a carer views or downloads a signed form, this action is recorded in the audit log with full attribution, consistent with the access-event logging applied to patients accessing their own records.

Aftercare & Follow-Ups

Aftercare is delivered in the correct patient context and may be visible to the guardian within their permission set. AI-first interactions are supported with escalation pathways. Escalations always retain full patient attribution, with dual `PatientId` / `CarerId` attribution supplied to Aftercare Manager as described in §4.1.

Contextual "Acting As" Enforcement

All surfaces that render delegated data MUST display a clear, persistent indicator: **"You are acting on behalf of [Patient Name]."** There is no anonymous or shared access. All delegated actions are attributed to the acting user; the represented patient is always explicitly recorded.

Example audit entry: *"Medical history for Emily Doe submitted by Jane Doe (Guardian)"*

4.3 Age-Based Transition to Independence

Family Profiles support automatic transition at a configurable age threshold (default: 18). At the threshold:

- The patient is invited to create their own independent account
- Guardian access is revoked automatically
- All parties (patient and guardian) are notified via Communication Hub
- The transition event is logged in the audit trail

The age threshold is configurable by practice administrators.

5. Delivery Surfaces & Access (Authoritative)

5.1 Web Portal

Staff access family relationship management, consent verification, and full audit visibility from the staff web portal. Relationship creation, modification, suspension, and revocation are performed here. The staff web portal also surfaces care plan entitlement status for dependants where the practice uses Care Plan Subscriptions — staff may view which plan a dependant is enrolled on and what entitlements are active, drawing from the entitlement data consumed from Care Plan Subscriptions (see §6.1).

5.2 Tablet App

The tablet surface is read-only for family awareness. Execution of actions (booking, form signing) remains patient-specific and is not performed from the tablet context.

5.3 Patient Mobile App

The patient mobile app surfaces a profile switcher allowing authenticated users to move between their own record and Active linked dependant profiles. Delegated notifications, tasks, and actions are presented in the correct patient context. The acting-as indicator is always visible when in a delegated session.

5.4 Engagement Signals

Family Profiles emits engagement signals for staff visibility, including: number of active family profiles per practice, pending invite redemptions, age-transition events due or overdue, and delegated action counts by relationship type. These signals are available to the staff web portal and to any connected analytics surface.

6. Integration Contracts

6.1 Inbound (this module consumes from)

From module	What	Contract
Appointment Manager	Offer lifecycle states (broadcast, lock window, confirmed, expired) for delegated waitlist participation	Synchronous rule enforcement
Digital Forms	Form version and completion state for attribution capture	Event / async
Dentally (PMS)	Responsible-party data for suggested link discovery (optional)	Read-only, async
Access Manager	Role and permission set definitions; grant lifecycle acknowledgements for guardian and proxy access	Synchronous
Communication Hub	Delivery confirmation for invite and transition notifications	Event
Care Plan Subscriptions	Care plan membership and entitlement status for dependants, for display in the staff web portal and to support family entitlement views	Event / async, read-only

6.2 Outbound (this module emits to)

To module	What	Contract
Appointment Manager	Delegated booking and cancellation actions, with acting-user attribution	Synchronous

Digital Forms	Delegated form completion and guardian signature events, including SigningRole, CarerId, and SignedByUserId for attribution	Synchronous
Aftercare Manager	Family context for correct patient-attributed aftercare delivery, including dual PatientId / CarerId attribution for escalated records	Event
Communication Hub	Notification triggers (invite, transition, revocation, confirmation)	Event
Task Manager	Task generation for staff follow-up on pending invites or transitions	Event
Integrated Payments	Payer attribution for delegated payment actions	Event
Access Manager	Permission grant creation, update, and revocation events aligned to Family Profile lifecycle transitions	Synchronous

6.3 PMS Boundary

Dentally is the external clinical system of record. Family Profiles reads Dentally responsible-party data solely for optional link-discovery suggestions. Family Profiles never writes to Dentally and never exposes Dentally clinical notes through any delegation surface. All clinical data remains in Dentally; Family Profiles governs only the relationship layer within Primoro.

7. AI Boundaries (Non-Negotiable)

AI MAY:

- Highlight potentially unlinked dependants and prompt staff to suggest Family Profiles
- Summarise family relationship status for staff review
- Support AI-first Aftercare interactions within an active delegated session, with escalation pathways retaining full patient attribution

AI MAY NOT:

- Create, approve, or activate any family relationship link
- Assign or modify permission sets
- Override or bypass consent requirements
- Auto-respond to waitlist offers on behalf of a delegated user

- Make commitments on behalf of the practice or a guardian
- Replace required human approval for any governed state transition

8. Audit & Compliance

The system MUST log:

- Family Profile creation, including consenting actor, method, and timestamp
- All state transitions (Created → Active, Modified, Suspended, Revoked/Archived) with actor and timestamp
- Link modification events (member additions, removals, permission changes)
- All delegated actions: booking, form completion, guardian signature, aftercare interaction — with acting user and represented patient recorded on every event
- Carer access to, or download of, signed form records — with full attribution
- Consent revocation events
- Age-based transition events, including notification dispatch
- All AI suggestions surfaced to staff, including which were accepted or rejected
- Access Manager permission grant creation, update, and revocation events triggered by this module
- Aftercare escalation events initiated in a delegated session, with dual PatientId / CarerId attribution

Audit logs MUST be immutable, append-only, and exportable for inspection by authorised staff and for regulatory review. No audit record may be modified or deleted once written.

9. Access Control

Access is governed via **Access Manager** using role-based permission sets scoped per relationship. There is no implicit access inheritance — every permission must be explicitly granted.

Action	Role(s) permitted
Create / initiate Family Profile	Staff (authorised)
Redeem invite / confirm consent	Guardian (authenticated in patient app)
Modify members or permissions	Staff (authorised)
Suspend or revoke profile	Staff (authorised)
View delegated patient data	Delegated user, within permission set
Complete forms / sign as guardian	Delegated user, within permission set
Download signed form records	Delegated user, where explicitly authorised
View full audit log	Staff (authorised)

View dependant care plan entitlements	Staff (authorised); delegated user, within permission set

- Removal from a Family Profile revokes delegated access immediately
- Staff access is always scoped and logged
- All sensitive operations (revocation, permission modification) MUST be confirmed before commit; the spec does not yet specify whether MFA step-up is required for these operations — see §15 Open Questions.

10. Integration Summary

- **Appointment Manager** — inbound rule enforcement for delegated booking and waitlist participation; outbound delegated booking actions
- **Digital Forms** — inbound form state for attribution; outbound delegated completion and guardian signature events with SigningRole, CarerId, and SignedByUserId
- **Aftercare Manager** — outbound family context for patient-attributed aftercare delivery, with dual PatientId / CarerId attribution for escalated records
- **Communication Hub** — outbound notification triggers for invites, transitions, and confirmations
- **Task Manager** — outbound task generation for staff follow-up on pending or transitioning profiles
- **Integrated Payments** — outbound payer attribution for delegated payment actions
- **Access Manager** — RBAC for all read/write/approve operations within this module; inbound permission set and grant lifecycle; outbound grant creation, update, and revocation events
- **Dentally (PMS)** — inbound read-only responsible-party data for optional link-discovery suggestions
- **Care Plan Subscriptions** — inbound read-only care plan membership and entitlement data for dependants, for display in staff and delegated views

11. Explicit Non-Goals

- **Merging patient records** — Family Profiles links records; it never merges them. Record consolidation is out of scope.
- **Exposing clinical notes or diagnoses** — clinical data remains in the PMS; no delegation surface exposes staff-only clinical content.
- **Bypassing consent** — no mechanism exists within this module to create an active delegation without explicit consent.
- **Billing logic or household ledger** — payer attribution is emitted to **Integrated Payments**, which owns all payment logic.
- **Messaging transport** — notification routing is triggered by this module but delivered by **Communication Hub**.
- **Governance Reporting** — consent and delegation audit exports for compliance reporting are a planned extension, not MVP scope.

12. Versioning & Governance

This specification is owned by: the Family Profiles module owner.

Changes to this spec require:

- Review by the MVP module owner
- Impact analysis across all declared related modules
- Version bump (patch / minor / major depending on scope of change)

All future changes must:

- Preserve individual patient record integrity
- Maintain explicit consent as a prerequisite for any active delegation
- Keep all delegated actions auditable with full actor attribution
- Respect the separation of concerns established in §2

13. Build Contract (Engineering & QA)

13.1 Canonical Data Model

```
family_profile (
 family_profile_id     UUID PRIMARY KEY,          -- immutable
 created_by            UUID NOT NULL,             -- staff user
 created_timestamp     TIMESTAMPTZ NOT NULL,
 status                ENUM(created, active, modified, suspended, revoked) NOT NULL,
 revoked_timestamp     TIMESTAMPTZ
)

family_member (
 family_member_id      UUID PRIMARY KEY,
 family_profile_id     UUID NOT NULL REFERENCES family_profile,
 patient_id            UUID NOT NULL,             -- FK to patient record
 acting_user_id        UUID NOT NULL,             -- FK to authenticated user
 role                  ENUM(primary_account_holder, parent_guardian, carer, dependant) NOT NULL,
 permission_set_id     UUID NOT NULL,             -- FK to Access Manager permission set
 status                ENUM(active, pending, revoked) NOT NULL,
 revoked_timestamp     TIMESTAMPTZ
)

family_audit_log (
 audit_id              UUID PRIMARY KEY,
 family_profile_id     UUID NOT NULL REFERENCES family_profile,
 event_type            TEXT NOT NULL,
 actor_user_id         UUID NOT NULL,
 represented_patient_id UUID,
 event_timestamp       TIMESTAMPTZ NOT NULL,
 payload               JSONB NOT NULL             -- immutable, append-only
)
```

13.2 Core Behaviour Rules

1. A Family Profile MUST NOT become Active until explicit consent has been confirmed and recorded with actor, method, and timestamp.
2. All delegated actions MUST record the acting user ID and the represented patient ID; neither may be null.

3. Removal of a family member MUST revoke their delegated access in the same transaction — no grace period.

4. A delegated user's waitlist offer engagement window MUST equal the window applied to direct patients; the system MUST NOT extend it.

5. Carer read or download of a signed form MUST generate an audit log entry with full attribution before the response is returned.

6. A Family Profile in Revoked/Archived state MUST NOT be transitioned back to Active; a new profile must be created.

7. Patient records MUST remain isolated — no cross-patient data may be returned through any delegation surface.

8. The acting-as indicator MUST be present on every delegated session surface; the system MUST NOT render delegated data without it.

9. Age-based transition MUST revoke guardian access automatically at the configured threshold and MUST dispatch notifications to all parties via Communication Hub before the revocation is finalised.

10. AI suggestions surfaced to staff (e.g. potential unlinked dependants) MUST be logged with their outcome (accepted / dismissed) in the audit log.

11. Delegated form signing events MUST include a valid `SigningRole` value (`Parent`, `LegalGuardian`, or `AuthorisedCarer`) derived from the delegating family member's `role` field; the system MUST NOT emit a signing delegation event where the Family Profile is not in Active state.

12. Aftercare escalation events initiated in a delegated session MUST supply both `PatientId` and `CarerId` as distinct fields to Aftercare Manager; neither may be null in a delegated context.

13. Access Manager permission grants corresponding to a Family Profile MUST be created or updated synchronously on profile activation or modification, and revoked in the same transaction as profile revocation.

14. Care plan entitlement data consumed from Care Plan Subscriptions MUST be treated as read-only; Family Profiles MUST NOT write to or modify entitlement records.

13.3 Configuration Surfaces

Configurable by practice administrators (Admin Control Plane):

- Permitted relationship roles (subset of the Role enum)
- Default permission sets per role
- Invite and verification rules (expiry window, redemption limits)
- Age-based transition threshold (default: 18)
- Maximum dependants per guardian (optional cap)

13.4 Filtering & Views

Staff views MUST support filtering by:

- Family Profile status (Created / Active / Suspended / Revoked)
- Relationship type (Guardian, Carer, Dependant)
- Age-transition state (upcoming, overdue, completed)
- Pending invites awaiting redemption
- Audit events (by event type, actor, or date range)

13.5 Module Extension Map

This contract is designed to accommodate the following future extensions without requiring breaking changes:

- **Governance Reporting** — consent and delegation audit exports, drawing from the existing immutable audit log
- **Group Controls** — cross-site consistency for multi-site practices, using the existing permission-set model
- **AI Guardian** — misuse or risk detection layer, reading from audit log signals with no write access to the profile object

13.6 Acceptance Criteria

The build of Family Profiles is complete when:

- [ ] All canonical objects (Family Profile, Family Member, Audit Log) can be created, read, and updated through the API
- [ ] State machine transitions enforce all rules in §3.2 (including irrevocability of Revoked state)
- [ ] Delegated booking works correctly and all Appointment Manager rules are enforced without modification
- [ ] Guardian form signing is attributed with actor, represented patient, form version, and timestamp; correct `SigningRole`, `CarerId`, and `SignedByUserId` values are supplied to Digital Forms on every delegated signing event
- [ ] Delegated waitlist offer engagement respects the Appointment Manager engagement lock window — no extension granted
- [ ] Carer form view and download is gated by permission set and generates a fully attributed audit log entry
- [ ] Aftercare is delivered in the correct patient context with guardian visibility governed by permission set; dual `PatientId` / `CarerId` attribution is present on all escalated aftercare records
- [ ] Access revocation is immediate and transactional with member removal; corresponding Access Manager grants are revoked in the same transaction
- [ ] Age-based transition revokes guardian access at threshold and dispatches notifications via Communication Hub
- [ ] Full audit trail is available for all events listed in §8
- [ ] All integrations in §6 are wired and tested, including Care Plan Subscriptions (read-only entitlement data) and the Access Manager grant lifecycle
- [ ] AI boundaries in §7 are enforced (negative tests pass — AI cannot create links or assign permissions)
- [ ] Access control is enforced per §9, including no implicit access inheritance
- [ ] All non-functional requirements in §14 are met

14. Non-Functional Requirements

- **Performance:** Family profile switching MUST be instantaneous from the user's perspective. Delegated session context resolution MUST complete within 300 ms at the 95th percentile under normal practice load. No cross-patient data leakage is permitted at any latency.
- **Reliability:** No orphaned link records — partial failures during creation or revocation MUST be recovered cleanly, leaving the profile in a consistent state. The module MUST degrade gracefully if Communication Hub is unavailable during a transition event, queuing notifications for delivery rather than blocking the state change.

- **Scalability:** The module MUST support multi-site, multi-tenant operation. A single guardian may be linked to dependants across multiple practices without cross-tenant data exposure.
- **Security:** Encryption at rest and in transit is required for all profile and audit data. Permission set checks MUST be enforced server-side on every delegated API request; client-side gating alone is not sufficient.
- **Privacy:** GDPR-aligned data retention applies to all Family Profile records and audit logs. Consent is the lawful basis for all delegated access; revocation of consent MUST be honoured immediately. Data subject access requests and right-to-erasure requests involving delegated records must be handled in coordination with the practice's data controller obligations; the audit log is retained per regulatory retention requirements even where other profile data is erased.
- **Observability:** The module MUST export metrics including: active profile count, pending invite count, revocation rate, age-transition events fired, and delegated-action volume by type. Structured logs MUST be emitted for every state transition and delegated action. Distributed traces MUST span delegated booking and form-completion flows into Appointment Manager and Digital Forms respectively.
- **Accessibility:** The acting-as indicator and profile switcher MUST meet WCAG 2.1 AA standards. The indicator MUST be perceivable without relying on colour alone.

15. Open Questions

> Outstanding decisions before this spec can be promoted from `draft` to `published`.

1. **MFA for sensitive operations:** The original spec does not specify whether MFA step-up is required for high-risk staff actions (revocation, permission modification). This needs a decision before build.
2. **Invite expiry and redemption limits:** The original notes that invite and verification rules are configurable but does not specify default expiry windows or maximum redemption attempts. Defaults must be defined.
3. **Maximum dependants per guardian:** The original notes this is configurable "if required" but does not specify a default cap or whether a hard maximum exists. The product team needs to decide whether a default cap ships with MVP.
4. **Suspended state behaviour:** The original defines Suspended as a lifecycle state but does not specify what delegated access is permitted (if any) while a profile is suspended, or who may reinstate it. This needs explicit definition.
5. **GDPR erasure and audit log retention:** Where a patient exercises a right-to-erasure request, the interaction between erasure and the immutable audit log is not resolved in the original. The retention policy for audit records referencing erased subjects needs a legal/compliance decision.
6. **SigningRole mapping for edge cases:** Digital Forms' `SigningRole` enum includes `LegalGuardian` as distinct from `Parent`. The mapping from the `parent_guardian` role enum value to one or the other is not yet defined; a decision is needed on whether this distinction is captured at the Family Profile level or supplied ad hoc at signing time.
7. **Care Plan entitlement display scope:** It is not yet decided whether delegated users (guardians/carers) may view a dependant's care plan entitlement status in the patient mobile app, or whether this view is restricted to the staff web portal. The product team must confirm the intended scope before build.