Security and Privacy

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

Security and Privacy – Technical Specification

1. Module Purpose & Scope (Authoritative)

Security and Privacy is the platform-wide, non-optional foundation of Primoro. It protects patient and staff data by default, removes common real-world security failure points (shared logins, lost devices, poor off-boarding), and ensures every action is attributable, auditable, and revocable. It operates quietly in the background across every device and workflow — built in, not bolted on.

It governs:

- Platform-wide privacy-by-design controls and secure defaults across all Primoro surfaces (Patient App, Staff App Mode, In-Practice Tablets, Web Portal)
- Data encryption in transit and at rest, device-aware session protection, and prevention of casual data leakage
- Audit logging for all access, activity, and data interaction in support of GDPR, NHS DSPT, and healthcare inspection requirements

It explicitly does not:

- Define identity lifecycle, role assignments, or RBAC logic — owned by Access Manager
- Orchestrate messaging or notification content — owned by Communication Hub
- Execute business logic or clinical workflows — owned by individual feature modules and PMS
- Surface analytics or reporting — owned by Smart Dashboards

Security and Privacy governs *how* data is protected and accessed, not *what* actions occur.

2. Ownership & Responsibilities

2.1 Security and Privacy IS Responsible For

- Platform-wide privacy-by-design controls: minimum data exposure, least-privilege access, secure defaults
- End-to-end data protection across all Primoro surfaces: Patient App, Staff App Mode, In-Practice Tablets, Web Portal
- Secure authentication and session handling in coordination with Access Manager
- Data encryption in transit (TLS 1.2+, certificate pinning) and at rest (OS-managed keystores and backend encrypted storage)
- Device-aware and context-aware protection including auto-lock, session wipe on shared tablets, and notification privacy
- Prevention of casual data leakage: screenshot blocking, screen-recording blocking, clipboard controls, app-switcher content masking

- Controlled document viewing and sharing via Document Hub integration (time-limited links, access logging, automatic revocation)
- Audit logging of all access, activity, data interaction, and AI activity across the platform
- Supporting compliance alignment with UK GDPR, NHS DSPT, Cyber Essentials, ISO/IEC 27001-aligned controls, and SOC 2

2.2 Security and Privacy IS NOT Responsible For

- Identity lifecycle management, RBAC definition, or permission assignment — owned by Access Manager
- Messaging orchestration or notification content decisions — owned by Communication Hub
- Business logic and clinical workflows — owned by individual feature modules
- Clinical decision-making — owned by PMS
- Analytics and reporting surfaces — owned by Smart Dashboards

3. Core Objects (Normative)

3.1 SecurityEvent (Canonical Artefact)

A SecurityEvent is the platform's single, authoritative, immutable audit record representing one attributable action. It is the base model that all other modules' audit event types extend or map to. Document Hub's AuditEvent, AI Assistant (Aiden)'s AuditEvent, and Admin Control Plane's admin-action audit records are all specialisations of this shape — they MUST include every required field listed below and MAY add module-specific fields in the `payload` JSONB column. No module may define a parallel, incompatible audit record type; all audit obligations MUST resolve to a SecurityEvent emitted to the platform audit sink.

Minimum required fields:

- EventId
- EventType (enumerated — see §3.2)
- Actor (User | System | AI)
- Target (User | Document | Record)
- DeviceId — required on all events; for AI Assistant (Aiden) events this field correlates the audit record with the device session in which the interaction occurred, maintaining the same attribution guarantee as all other platform events
- Timestamp
- RepresentedPatientId *(optional)* — populated when the Actor acts on behalf of a different patient (e.g. a guardian submitting on behalf of a dependent, or a family-profile delegated user acting on behalf of a linked patient); enables full attribution of delegated actions across all surfaces
- DelegationRole *(optional)* — the role under which delegation was granted (e.g. `Guardian`, `AuthorisedCarer`); recorded alongside `RepresentedPatientId`

Delegated-action attribution. Where a family-profile relationship or any other delegation grants a user authority to act on behalf of a patient, every resulting SecurityEvent MUST populate both `RepresentedPatientId` and `DelegationRole`. This ensures the audit record reads unambiguously — for example: *"Medical history for Emily Doe submitted by Jane Doe (Guardian)"* — and satisfies the immutable, append-only attribution requirement mandated by Family Profiles and by the platform's GDPR obligations. The audit log MUST be filterable by `RepresentedPatientId` (see §13.4) so that all delegated actions for a given patient can be retrieved for

inspection or subject-access requests.

Admin-action attribution. All administrative actions performed via the Admin Control Plane MUST be emitted as SecurityEvents with a named Actor, a specific EventType (see §3.2), and all required fields populated. This satisfies Admin Control Plane's mandate that every admin action is fully auditable. The Audit & Compliance module consumes these events from the platform audit sink; Security and Privacy is the authoritative producer and schema owner.

AuditEvent alignment. Modules that define their own AuditEvent model (e.g. Document Hub, AI Assistant (Aiden)) MUST treat SecurityEvent as the canonical base. Any additional fields defined by a consuming module are additive only and MUST be carried in the `payload` field. Immutability, tamper-evidence, and exportability guarantees defined in §8 apply equally to all specialised AuditEvent records.

3.2 EventType Enumeration (Authoritative)

Modules MUST map their audit obligations to one of the values below. Where a module's event fits no existing type, it MUST use the most specific applicable type and MAY attach a `SubType` string for further classification.

EventType	Description
`Login`	Successful user authentication
`Logout`	Explicit or automatic session termination
`MFAChallenge`	MFA challenge issued and result recorded (pass or fail)
`RoleChanged`	Role or permission assignment added, modified, or removed
`View`	PHI or sensitive record accessed or viewed
`Share`	Content shared with an internal or external party
`Revoke`	Access, share, or token revoked
`Delete`	Record, document, or data deleted
`Escalation`	Privilege escalation requested or granted
`SupportSessionGranted`	JIT elevated support-access session opened (records `SessionId`, `TenantId`, `ApprovedBy`, `ExpiresAt`)
`SupportSessionExpired`	JIT support-access session reached its time limit and was automatically closed
`TrayReady`	Nurse confirmed a decontamination tray as ready on a shared tablet

`TaskCompleted`	Individual work-package task marked complete on a shared tablet, attributed to the named user
`WorkflowCompleted`	End-of-workflow completion marker (e.g. Finish & Send) recorded on a shared tablet
`FormAssigned`	Digital form assigned to a patient or staff member
`FormAccessed`	Patient or staff member opened an assigned form
`FormSubmitted`	Form submitted by the completing party
`FormSigned`	Signature captured on a form
`FormReviewed`	Staff member reviewed a completed form
`FormDeclined`	Form declined or rejected by staff or patient
`FormExpired`	Assigned form reached its expiry without completion
`DashboardAccessed`	A dashboard or dashboard view was opened by a user
`ActionLaunched`	A workflow action was triggered from a dashboard
`EvidenceClipRetained`	An ambient-audio evidence clip was created and stored under governed conditions (see §4.7)
`CaptureZoneActivated`	An ambient-audio or camera-event capture zone was activated or deactivated (see §4.7)
`RecordingStarted`	A meeting or consultation recording session was initiated
`RecordingExpired`	A meeting or consultation recording reached its configured retention expiry and was destroyed
`VoiceProfileCreated`	A speaker voice profile was created for meeting attribution purposes
`VoiceProfileDeleted`	A speaker voice profile was deleted or expired
`DelegatedActionPerformed`	An action was performed by a delegated user acting on behalf of a represented patient (populated alongside `RepresentedPatientId` and `DelegationRole`)

All `SupportSession*` events MUST record `SessionId`, `TenantId`, `ApprovedBy`, and `ExpiresAt` in the event payload to satisfy the Admin Control Plane audit requirement for time-boxed elevated access.

There is no state machine applicable to SecurityEvent itself — events are write-once and immutable by definition. State machine modelling applies to governed objects in feature modules that emit SecurityEvents on transition.

4. Core Security Capabilities

4.1 Privacy by Design (Non-Negotiable)

The module MUST enforce:

- Minimum data exposure at every layer
- Least-privilege access by default
- Data visible only when contextually required
- Secure defaults everywhere — no reliance on user "best practice" behaviours

The module MUST apply defence in depth: secure identity and authentication, role-based access enforcement, device-level controls, encrypted storage and transport, session management and auto-logout, and audit and anomaly monitoring. No single control is relied upon in isolation.

4.2 Authentication & Identity Security (Authoritative)

Patients

The module MUST enforce:

- Passwordless login by default (OTP)
- Secure token storage in OS keystore
- Automatic session expiry and re-verification

The module MAY support:

- Optional biometrics for convenience

Staff

The module MUST enforce:

- A hidden staff-mode activation gesture required before any authentication screen is presented — this acts as a security boundary that prevents patients from inadvertently discovering or accessing Staff App Mode
- Enterprise SSO (Microsoft Entra ID / Google Workspace)
- MFA inherited from the identity provider
- Short-lived access tokens with role-scoped sessions
- Immediate revocation for leavers and locums

4.3 Session & Device Protection (Authoritative)

Personal Devices (Staff & Patients)

The module MUST enforce:

- Encrypted local storage
- Biometric-protected secure tokens
- App auto-lock after inactivity

- No inclusion in OS cloud backups
- Secure notification handling with no sensitive content in previews

Shared Clinic Tablets

The module MUST enforce:

- Mandatory user authentication before session start
- Automatic logout on inactivity or rota end time
- Full data wipe between users — no persistent patient data between sessions

The module MAY support:

- Fast login mechanisms (badge / PIN / QR) for operational efficiency

Screenshot, Screen Recording & Clipboard Protection

The module MUST enforce:

- Blocking of screenshots and screen recordings on screens displaying sensitive data
- App content hidden in the OS app switcher
- Controlled clipboard copying with user-visible warnings
- Document viewers disabling local export by default

4.4 Documents & Media Security (Authoritative)

The module MUST enforce:

- Secure, streamed document viewing with no local export by default
- Time-limited, revocable access links
- No email attachments containing PHI
- Annotations stored separately from originals
- Access logging for every view, download, and share event
- Automatic share revocation on document update or deletion

4.5 Data Encryption

In Transit

The module MUST enforce:

- TLS 1.2+ for all communication
- Certificate pinning for critical endpoints
- Secure notification payloads with no PHI exposed

At Rest

The module MUST enforce:

- Encrypted storage on device via OS-managed keystores
- Encrypted storage in backend systems
- File hashes and integrity checks

- No plaintext sensitive data persisted anywhere

4.6 Privacy Controls & User Rights

The module MUST support:

- Clear privacy notices on first use
- Consent capture where required by regulation
- Opt-in analytics and telemetry
- Notification privacy controls
- Right of access (data export) aligned to UK GDPR
- Right to erasure — GDPR-aligned deletion including full local wipe on account deletion

4.7 Ambient Audio and Camera-Event Capture (Authoritative)

Where AI features (such as AI Quality Monitor) process ambient audio or camera-event inputs, the following controls apply without exception.

The module MUST enforce:

- **No raw audio storage by default.** Raw audio is processed in-memory and discarded immediately after inference. Persistent storage of raw audio is prohibited unless an evidence clip is explicitly required under a governed quality or safety workflow.
- **Evidence clip controls.** Short, time-bounded audio clips MAY be retained only where a governed quality or safety workflow explicitly requires an evidence record. Clips MUST be: time-limited in duration; stored encrypted at rest; access-controlled to authorised reviewers only; subject to automatic expiry according to the retention policy configured for the practice; and logged as a distinct `EvidenceClipRetained` audit event.
- **Camera-event inputs** (e.g. decontamination or clinical workflow triggers) are treated as structured event data rather than raw video. No raw video frames are persisted. Derived event data is subject to the same RBAC, encryption, and audit requirements as all other platform data.
- All ambient-capture processing is auditable end-to-end, including activation, inference, clip creation, clip access, and clip deletion.

Zone-based capture activation and consent. AI Quality Monitor and any other module that operates zone-configured ambient audio or camera-event monitoring introduces additional obligations that Security and Privacy co-governs:

- **Capture zone activation** MUST be logged as a `CaptureZoneActivated` SecurityEvent, recording the zone identifier, the activating actor, the capture modality (audio | camera-event), and the timestamp. Deactivation MUST be similarly logged.
- **Consent gates.** Before any capture zone is activated in a space accessible to patients, a practice-configured consent notice MUST be presented (e.g. in-room signage, on-screen disclosure, or both) in accordance with UK GDPR Article 13 transparency requirements. Security and Privacy enforces that no capture zone may be moved to an active state without the consent configuration being present and logged. The specific signage format is owned by the AI Quality Monitor module; the enforcement gate is owned here.
- **Staff disclosure.** Staff operating in a monitored zone MUST have been notified via the platform's staff notice mechanism. Security and Privacy enforces that the zone activation audit trail includes confirmation that the staff disclosure obligation has been satisfied.

- Zone configuration changes (adding, modifying, or removing a zone) MUST themselves be logged as SecurityEvents with the configuring actor identified.

4.8 Meeting and Consultation Recordings (Authoritative)

Where AI features (such as AI Meeting Notes) capture recordings of meetings or consultations, the following controls apply without exception. These complement the general ambient-capture rules in §4.7 and address the specific privacy considerations arising from structured meeting recordings, live transcription, and speaker voice profiling.

The module MUST enforce:

- **Explicit capture activation.** Recording MUST NOT begin without an explicit, attributed activation event logged as a `RecordingStarted` SecurityEvent, recording the meeting identifier, the activating actor, the participating parties, and the surface on which recording is occurring. Implicit or background-only recording is prohibited.
- **Participant transparency.** All participants (staff and patients) present in a recorded session MUST be notified that recording is active before or at the point of capture, in compliance with UK GDPR Article 13 and any applicable employment law obligations for staff. The notification mechanism is owned by the AI Meeting Notes module; the enforcement gate — that no recording may proceed without the notification obligation being discharged — is owned here.
- **Voice profile governance.** Where speaker attribution relies on voice profiles, the creation and deletion of each voice profile MUST be logged as `VoiceProfileCreated` and `VoiceProfileDeleted` SecurityEvents respectively, attributed to the actor who authorised or triggered the action. Voice profiles constitute personal biometric data under UK GDPR and MUST be: stored encrypted at rest; access-controlled to authorised staff only; retained only for the period necessary for attribution purposes; and subject to the same right-of-erasure obligations as other personal data (subject to the audit-log immutability tension noted in §15, Open Question 6).
- **Retention and expiry.** Recordings MUST be retained only for the period configured by the practice (default period to be defined — see §15, Open Question 1). On expiry, recordings and derived transcripts MUST be destroyed and the destruction MUST be logged as a `RecordingExpired` SecurityEvent. Organiser-initiated early expiry decisions MUST similarly be logged.
- **Data minimisation.** Raw audio from recordings MUST NOT be retained beyond the configured retention window. Derived transcript and structured note data are subject to the same RBAC, encryption, and audit requirements as all other platform PHI.
- **No cross-tenant learning.** Voice profiles and recording-derived data MUST NOT be used for model training or shared across customer tenants under any circumstances.

4.9 Access Manager Attribution Contract (Authoritative)

Security and Privacy and Access Manager share a joint responsibility for ensuring that every action on the platform is attributed to a named, authenticated actor. The following constraints govern the boundary between the two modules:

- Access Manager is the authoritative source of identity, role state, and session validity. Security and Privacy consumes this state and enforces it at the session, device, and data layers.
- No shared or anonymous accounts are permitted on any Primoro surface. This constraint is enforced jointly: Access Manager prevents their creation; Security and Privacy prevents their use by refusing to issue or honour tokens that do not carry a named, attributed actor identity.

- Shared-device session management (mandatory auth, auto-logout, full wipe between users) is enforced by Security and Privacy using session state signals received from Access Manager. Where Access Manager signals a session end (e.g. role revocation, leaver off-boarding, rota-end auto-logout), Security and Privacy MUST treat this as an immediate, global revocation across all active surfaces.
- All authentication events, session events, and role-change events originating in Access Manager MUST be logged as SecurityEvents by Security and Privacy, with the Access Manager event as the source trigger. Access Manager does not write to the audit log directly; it emits events that Security and Privacy consumes and converts to SecurityEvents.

5. Delivery Surfaces & Access (Authoritative)

5.1 Web Portal

Security and Privacy controls are enforced transparently in the Web Portal. Staff sessions are scoped to authenticated roles, PHI screens block screenshot and recording, and all activity is audit-logged. No sensitive data is cached locally in the browser beyond session scope.

5.2 Tablet App (In-Practice Tablets)

Security and Privacy governs mandatory user authentication before any session, fast-login support (badge / PIN / QR), automatic logout on inactivity or rota end, and full data wipe between users. No patient data persists between sessions.

5.3 Patient Mobile App

Security and Privacy governs passwordless OTP login, optional biometrics, encrypted local storage, app auto-lock, and notification privacy controls. Account deletion triggers a full local wipe.

5.4 Staff App Mode

Security and Privacy governs the hidden activation gesture as a security boundary, SSO and MFA inheritance, role-scoped short-lived tokens, and immediate revocation on role change or departure.

5.5 Engagement Signals

Security and Privacy does not surface engagement signals directly to staff dashboards. Anomaly signals and audit summaries are consumed by Smart Dashboards via read-only integration; Security and Privacy does not own their presentation.

6. Integration Contracts

6.1 Inbound (this module consumes from)

From module	What	Contract
Access Manager	Role assignments, session state, and revocation events	Sync / event
AI Quality Monitor	Ambient audio inference triggers and zone activation signals	Internal API

AI Meeting Notes	Recording lifecycle events (start, expiry, voice profile create/delete) requiring audit logging	Event
Document Hub	Document access and share events requiring audit logging	Event
Family Profiles	Delegated-action events carrying `RepresentedPatientId` and `DelegationRole` for audit attribution	Event
Admin Control Plane	Admin configuration-change events requiring audit logging as SecurityEvents	Event

6.2 Outbound (this module emits to)

To module	What	Contract
Access Manager	Session state, revocation confirmations	Sync
Smart Dashboards	Audit and anomaly signals (read-only)	Event
Communication Hub	Notification privacy enforcement signals	Event
Document Hub	Time-limited link issuance and revocation	Sync
Audit & Compliance	All SecurityEvents (canonical audit sink)	Event

6.3 PMS Boundary

The PMS is responsible for clinical record storage and clinical decision-making. Security and Privacy does not govern PMS-internal data handling but enforces encryption, access control, and audit logging on all data that crosses into Primoro surfaces from the PMS boundary.

7. AI Boundaries (Non-Negotiable)

Module does not embed AI surfaces directly. AI features on the platform (e.g. AI Quality Monitor, AI Assistant, AI Meeting Notes) operate inside the Security and Privacy model under the following constraints.

AI MAY:

- Process ambient audio or camera-event inputs in-memory for inference
- Produce structured event data from camera triggers

- Retain time-bounded evidence clips where a governed quality or safety workflow explicitly requires it
- Capture structured meeting recordings under the consent and activation controls defined in §4.8
- Surface audit summaries for human review

AI MAY NOT:

- Store raw audio persistently except under the explicit evidence-clip governance defined in §4.7 or the meeting-recording governance defined in §4.8
- Store raw video frames under any circumstances
- Activate capture zones or begin recordings without explicit, attributed activation events and the applicable consent/notification obligations being discharged
- Bypass RBAC, encryption, or audit controls
- Make access or revocation decisions autonomously
- Share learning data, voice profiles, or recording-derived data across customer tenants
- Replace required clinical judgement

8. Audit & Compliance

The system MUST log the following events using the SecurityEvent model (§3.1) with the EventTypes defined in §3.2:

- All user authentication and session events (`Login`, `Logout`, `MFAChallenge`)
- All role and permission changes (`RoleChanged`, `Escalation`)
- All access to PHI or sensitive records (`View`, `Share`, `Delete`)
- All token and access revocations (`Revoke`)
- All JIT support-access session lifecycle events (`SupportSessionGranted`, `SupportSessionExpired`) — including `SessionId`, `TenantId`, `ApprovedBy`, and `ExpiresAt` in payload
- All shared-tablet workflow events (`TrayReady`, `TaskCompleted`, `WorkflowCompleted`)
- All form lifecycle events (`FormAssigned`, `FormAccessed`, `FormSubmitted`, `FormSigned`, `FormReviewed`, `FormDeclined`, `FormExpired`)
- All dashboard and action events (`DashboardAccessed`, `ActionLaunched`)
- All ambient-capture events including activation, inference, clip creation, clip access, and clip deletion (`EvidenceClipRetained`, `CaptureZoneActivated`)
- All meeting and consultation recording lifecycle events (`RecordingStarted`, `RecordingExpired`)
- All voice profile lifecycle events (`VoiceProfileCreated`, `VoiceProfileDeleted`)
- All delegated actions performed on behalf of a represented patient (`DelegatedActionPerformed`, with `RepresentedPatientId` and `DelegationRole` populated)
- All admin configuration-change events originating in the Admin Control Plane, logged with the configuring actor and timestamp

Audit logs MUST be immutable, tamper-evident, fully attributable to a named Actor, and exportable for regulatory inspection.

Audit logs MUST NOT be deletable by any application-layer user or process, including practice admins. Deletion or expiry of audit records, where legally permitted, MUST be governed by a system-level retention policy only.

Primoro's compliance alignment targets: UK GDPR and Data Protection Act, NHS Data Security & Protection Toolkit (DSPT), Cyber Essentials, ISO/IEC 27001-aligned controls, SOC 2 (security, availability, confidentiality). Alignment is architectural, not checklist-based.

9. Access Control

Security and Privacy enforces access control in coordination with Access Manager.

Role definitions and permission assignments are owned exclusively by Access Manager. Security and Privacy consumes role state from Access Manager and enforces it at the session, device, and data layer.

Operation	Who can perform
Read audit logs	Authorised practice admin roles (via Access Manager)
Configure authentication methods	Practice admin (Admin Control Plane)
Configure session timeout rules	Practice admin (Admin Control Plane)
Configure retention and deletion policies	Practice admin (Admin Control Plane)
Configure notification privacy defaults	Practice admin (Admin Control Plane)
Configure device-specific behaviour	Practice admin (Admin Control Plane)
Configure capture zones	Authorised practice admin roles (Admin Control Plane); activation logged as `CaptureZoneActivated`
Trigger evidence-clip access	Authorised reviewers only (access-controlled per §4.7)
Access meeting recordings and transcripts	Authorised staff only (access-controlled per §4.8)
Create or delete voice profiles	Authorised staff only; logged as `VoiceProfileCreated` / `VoiceProfileDeleted`
Revoke access or sessions	Access Manager (immediate and global)

MFA is inherited from the enterprise identity provider for all staff. MFA enforcement is a MUST for all staff authentication; it is not configurable off at the practice level.

10. Integration Summary

- **Access Manager** — bidirectional; role state and session state consumed inbound, session and revocation signals emitted outbound; RBAC enforced at all layers; all auth/session/role-change events logged as SecurityEvents by this module (see §4.9)
- **Communication Hub** — outbound notification privacy enforcement signals

- **Document Hub** — time-limited link issuance, revocation, and access audit logging; Document Hub's AuditEvent is a specialisation of the canonical SecurityEvent defined in §3.1
- **Smart Dashboards** — outbound read-only audit and anomaly signals
- **AI Quality Monitor** — inbound ambient audio inference triggers and zone activation signals; governed by §4.7 and §7
- **AI Assistant (Aiden)** — subject to AI boundaries in §7; RBAC respected at all times; AI activity fully auditable; Aiden's AuditEvent is a specialisation of the canonical SecurityEvent (§3.1) with `DeviceId` correlating to the session device
- **AI Meeting Notes** — inbound recording lifecycle events; governed by §4.8 and §7; voice profile data governed as biometric personal data
- **Family Profiles** — inbound delegated-action events; `RepresentedPatientId` and `DelegationRole` populated on all SecurityEvents arising from delegated access
- **Admin Control Plane** — inbound admin configuration-change events; all admin actions emitted as SecurityEvents to the platform audit sink; Audit & Compliance ingests from the same sink
- **Patient App** — security controls applied: OTP, biometrics, encrypted storage, notification privacy
- **Staff App Mode** — security controls applied: hidden activation gesture, SSO, MFA, role-scoped tokens, immediate revocation
- **In-Practice Tablets** — security controls applied: mandatory auth, auto-logout, session wipe

11. Explicit Non-Goals

- MDM or managed-device requirement — Primoro does not require or depend on MDM solutions
- Staff-training-only security — security enforcement is architectural; it does not rely on user behaviour
- Raw storage URL exposure — never exposed to any client surface
- Shared or anonymous access — explicitly prohibited platform-wide
- Trading security for convenience — not in scope under any configuration

12. Versioning & Governance

This specification is owned by: Platform Engineering Lead.

Changes to this spec require:

- Review by the MVP module owner
- Impact analysis across all declared related modules (see /propose) — given that Security and Privacy underpins every module, all cross-module impacts must be assessed
- Version bump (patch / minor / major) depending on scope of change

13. Build Contract (Engineering & QA)

13.1 Canonical Data Model

```
security_event (
 event_id              UUID PRIMARY KEY,
```

```
 event_type            VARCHAR NOT NULL,        -- enumerated; see §3.2
 sub_type              VARCHAR,                 -- optional classifier
 actor_type            VARCHAR NOT NULL,        -- 'User' | 'System' | 'AI'
 actor_id              UUID NOT NULL,
 target_type           VARCHAR NOT NULL,        -- 'User' | 'Document' | 'Record'
 target_id             UUID NOT NULL,
 device_id             UUID,
 timestamp             TIMESTAMPTZ NOT NULL,
 represented_patient_id UUID,                   -- nullable; delegated action
 delegation_role       VARCHAR,                 -- nullable; e.g. 'Guardian'
 payload               JSONB                    -- event-specific fields
                                                -- (e.g. SessionId, TenantId,
                                                --  ApprovedBy, ExpiresAt
                                                --  for SupportSession* events;
                                                --  ZoneId, Modality for
                                                --  CaptureZoneActivated;
                                                --  MeetingId for Recording*;
                                                --  ProfileId for VoiceProfile*)
)
```

The `security_event` table MUST be append-only at the application layer. No UPDATE or DELETE operations on this table are permitted via application code paths.

13.2 Core Behaviour Rules

1. No shared accounts are permitted on any Primoro surface.
2. All sensitive actions are logged as SecurityEvents with a named Actor before the operation completes.
3. Tokens are short-lived and revocable; revocation takes effect immediately and globally.
4. Shared devices MUST never retain user data or patient data after session end; a full wipe is mandatory.
5. Screens displaying PHI MUST block screenshot and screen-recording attempts on all supported OS surfaces.
6. App content MUST be hidden in the OS app switcher on all mobile surfaces.
7. Certificate pinning MUST be active for all critical endpoints.
8. No plaintext sensitive data MUST be persisted at any storage layer.
9. Raw audio from ambient-capture AI features MUST be discarded immediately after inference unless an evidence clip is explicitly required by a governed workflow.
10. No raw video frames from camera-event AI features MUST be persisted under any circumstances.
11. All `SupportSession*` events MUST carry `SessionId`, `TenantId`, `ApprovedBy`, and `ExpiresAt` in the event payload.
12. Audit logs MUST be immutable and exportable; no application-layer process may delete or alter them.
13. Access revocation (role change, leaver, locum departure) MUST apply instantly and globally across all active sessions.
14. No capture zone MAY be activated without the consent/notification obligations in §4.7 being discharged and a `CaptureZoneActivated` SecurityEvent being emitted.
15. No meeting or consultation recording MAY begin without an explicit `RecordingStarted` SecurityEvent emitted with all required fields and the participant notification obligation discharged.
16. Voice profiles constitute biometric personal data and MUST be stored encrypted, access-controlled, and subject to right-of-erasure obligations; their creation and deletion MUST be logged as SecurityEvents.

17. All delegated actions MUST populate `RepresentedPatientId` and `DelegationRole` on the emitted SecurityEvent.

18. All admin configuration-change actions originating in the Admin Control Plane MUST be logged as SecurityEvents with the configuring actor and timestamp; no admin action is exempt from audit.

13.3 Configuration Surfaces

Practice admin (via Admin Control Plane) can configure:

- Authentication methods permitted for staff and patients
- Biometric enablement per device class
- Session timeout rules (inactivity threshold, rota-end auto-logout)
- Notification privacy defaults
- Retention and deletion policies (including evidence-clip expiry, meeting recording expiry, and voice profile retention)
- Device-specific behaviour (shared vs personal)
- Capture zone definitions and active/inactive state

All configuration changes to the above settings MUST themselves be logged as SecurityEvents with the configuring actor and timestamp recorded.

13.4 Filtering & Views

Audit log views MUST support filtering by: EventType, Actor, Target, DeviceId, date range, RepresentedPatientId, and DelegationRole. Saved views are not defined in this specification — needs definition (see §15).

13.5 Module Extension Map

New EventType values MUST be proposed via a spec change to this document and agreed before implementation. The `SubType` field provides a controlled extension point for finer classification within existing EventType values without requiring a schema change. New ambient-capture modalities (beyond audio and camera events) MUST be governed by an extension to §4.7 before implementation begins. New AI-feature recording modalities MUST be governed by an extension to §4.8 before implementation begins.

13.6 Acceptance Criteria

The build of Security and Privacy is complete when:

- [ ] Data is encrypted in transit (TLS 1.2+, certificate pinning active) and at rest (OS keystores and backend encrypted storage)
- [ ] Screenshots and screen recordings are blocked on all PHI-displaying screens across Patient App, Staff App Mode, and In-Practice Tablets
- [ ] App content is masked in the OS app switcher on all mobile surfaces
- [ ] Access revocation applies instantly and globally across all active sessions
- [ ] Shared clinic tablets auto-logout and fully wipe session data on inactivity or rota end
- [ ] Audit trail captures every event defined in §8 and is immutable and exportable
- [ ] All EventType values in §3.2 are implemented and emittable
- [ ] `SupportSession*` events carry all required payload fields

- [ ] Raw audio is discarded after inference; evidence clips are only retained under the governed conditions in §4.7
- [ ] No raw video frames are persisted under any circumstances
- [ ] Capture zone activation and deactivation are logged as `CaptureZoneActivated` SecurityEvents and no zone may be activated without the consent gate being satisfied
- [ ] Meeting recording lifecycle events are logged (`RecordingStarted`, `RecordingExpired`) and no recording may begin without the participant notification obligation being discharged
- [ ] Voice profile creation and deletion are logged and voice profiles are stored encrypted with access controls applied
- [ ] All delegated actions populate `RepresentedPatientId` and `DelegationRole` in the SecurityEvent
- [ ] All admin configuration-change actions are logged as SecurityEvents
- [ ] All configuration changes by admins are themselves logged as SecurityEvents
- [ ] AI boundaries in §7 are enforced and negative tests pass
- [ ] Access control per §9 is enforced for all operations
- [ ] All non-functional requirements in §14 are met

14. Non-Functional Requirements

- **Performance:** Security controls MUST NOT introduce noticeable UI latency on any supported surface. Audit event writes MUST be non-blocking with respect to the primary user action that triggered them — write failures MUST queue and retry without blocking the user operation.
- **Reliability:** Security enforcement MUST remain fully active during partial outages. Audit logging MUST operate independently of feature module availability; if the audit sink is temporarily unavailable, events MUST be durably queued and replayed on recovery with no loss.
- **Scalability:** The SecurityEvent model MUST support multi-tenant isolation — one tenant's audit records MUST never be accessible to another tenant's application sessions. The design MUST accommodate multi-site practices under a single tenant.
- **Security:** Least-privilege enforced everywhere; defence-in-depth maintained across all layers; TLS 1.2+ in transit; OS-managed keystores and backend encryption at rest; no raw credentials or PHI in logs, metrics, or traces.
- **Privacy:** UK GDPR rights (access and erasure) MUST be honoured. Data retention policies MUST be configurable per practice. Account deletion MUST trigger full local wipe. Opt-in analytics only.
- **Accessibility:** Privacy notices, consent flows, and notification privacy controls MUST meet WCAG 2.1 AA accessibility standards.
- **Observability:** Security and Privacy MUST export: a count of SecurityEvents by EventType (metric); authentication failure rates by surface (metric); session revocation latency (metric); structured logs for all audit events; and distributed traces for cross-module security-enforcement paths. No PHI MUST appear in metrics, logs, or traces exported to observability tooling.

15. Open Questions

1. **Audit log retention period:** The original states that evidence-clip expiry follows "the retention policy configured for the practice" — but no default retention period or maximum retention cap is defined. This applies equally to meeting recordings and voice profiles. What is the platform-level default for each data type,

and is there a regulatory minimum or maximum that overrides practice configuration?

2. **Saved audit log views:** §13.4 notes that saved views for audit log filtering are not yet defined. What saved views are required for practice admin and inspector use cases?

3. **Anomaly monitoring:** §3.2 (Defence in Depth) names "audit and anomaly monitoring" as a security layer, but no anomaly detection logic, thresholds, or alerting contract is defined in the original. Is anomaly detection in scope for this module or deferred?

4. **Fast-login mechanisms on shared tablets:** Badge, PIN, and QR are listed as options. Which are mandatory to support at MVP, and which are optional?

5. **SOC 2 and ISO 27001 audit evidence:** The original states alignment is "architectural, not checklist-based." Is there a formal certification or audit engagement planned, and if so, by when? This may affect the audit export format required.

6. **Right to erasure and audit logs:** GDPR right to erasure is stated as in scope, but audit logs are required to be immutable. The tension between these two requirements — particularly where a patient requests erasure of records that appear as Targets in SecurityEvents, or where a staff member requests deletion of their voice profile — is unresolved.

7. **Capture zone consent format:** §4.7 requires that a consent notice be presented before any capture zone is activated in a patient-accessible space, but the specific format (in-room signage, on-screen disclosure, or both) is delegated to AI Quality Monitor. Should the minimum acceptable consent format be defined here as a platform-level standard, or remain module-configurable?

8. **Meeting recording participant notification:** §4.8 requires that all participants be notified before recording begins, but the notification mechanism is owned by AI Meeting Notes. Should Security and Privacy define a minimum notification standard (e.g. an in-app banner that must be acknowledged) to ensure the enforcement gate is unambiguous?