PRACTICE HARBOR · SECURITY DOCUMENTATION

Security Overview

System Description & Control Summary — Behavioral Health Practice Management Platform

Document version
1.0

Effective date
August 2026

Prepared by
Albert Wong, PhD — Security Official

Classification
Public

Operating entity
Somatopia, LLC (dba Practice Harbor)

Canonical source
practiceharbor.com/trust

Scope. This Security Overview describes the design of Practice Harbor's system, security controls, and HIPAA safeguards as of the effective date above, for use in vendor assessments and internal reviews. It is a self-attestation prepared by Practice Harbor management and is **not** an independent audit report. Full scope and limitations are stated in Section 15.

1. Company & Service Description

Practice Harbor is a behavioral-health practice management platform operated by Somatopia, LLC and founded by a licensed clinical psychologist. The platform provides scheduling, clinical documentation, insurance billing and claims (X12 837P/835), telehealth, secure client messaging, and a client portal to solo practitioners and small group practices. Protected health information (PHI) is processed in the platform's capacity as a HIPAA Business Associate to each customer practice.

2. System Boundaries & Infrastructure

The production system is self-hosted in a dedicated Amazon Web Services (AWS) account within the United States. AWS operates as a subservice organization under the AWS Business Associate Addendum; physical and environmental data-center controls are inherited from AWS and are outside the boundary of this description.

COMPONENT	TYPE	DESCRIPTION
Amazon ECS Fargate	Compute	Stateless containerized API/application servers
AWS Lambda	Compute	Event-driven asynchronous processing (bots, jobs)
Amazon Aurora PostgreSQL 16.11	Data store	FHIR R4 system of record; Multi-AZ; encrypted (KMS)
Amazon S3	Object storage	Binary documents/uploads/PDFs; server-side encryption
Amazon ElastiCache (Redis)	Cache	Ephemeral cache and rate-limit state; no PHI at rest
Amazon CloudFront	CDN / edge	TLS termination (min. TLSv1.2_2021); global delivery

COMPONENT	TYPE	DESCRIPTION
AWS WAF	Web app firewall	Application, front-end, and storage distributions
AWS Shield	DDoS protection	Network/transport-layer attack mitigation
AWS KMS	Key management	Encryption-key lifecycle for at-rest data
AWS CloudTrail / CloudWatch	Logging	Infrastructure audit and operational monitoring

3. Data Architecture & Records Management

The system of record is a FHIR R4 datastore on Amazon Aurora PostgreSQL 16.11 in a Multi-AZ configuration with storage-level AES-256 encryption under AWS KMS-managed keys, a 7-day automated backup window, and point-in-time recovery. Each FHIR resource type persists to a primary table and an append-only `<Resource>_History` table: every create, update, and delete produces an immutable, individually addressable version rather than an in-place overwrite, yielding a complete and reconstructable version lineage (prior field values and authoring identity) for every record. Application compute nodes are stateless and hold no PHI at rest. Records are maintained in the FHIR R4 open standard; complete structured exports are available on request, including upon service termination.

4. Encryption

- **At rest:** AES-256 across the Aurora PostgreSQL cluster and S3 object storage; keys managed by AWS KMS.
- **In transit:** TLS for all client and inter-service connections; minimum negotiated protocol TLSv1.2_2021 at the CloudFront edge; ACM-provisioned certificates.
- **Endpoints:** disk encryption on operational workstations.

5. Authentication & Session Management

- Passwords stored as bcrypt hashes; plaintext credentials never persisted.
- Sessions issued as asymmetrically signed JWTs (RS256/ES256): 1-hour access-token lifetime, rotating refresh token (2-week default).
- TOTP multi-factor authentication (RFC 6238) supported for practice accounts; enrollment offered at sign-in.
- API-layer request rate limiting; secrets held in managed secret storage, never in source code.

6. Authorization & Access Control

Authorization is evaluated server-side on every request against a per-membership AccessPolicy. Reads and writes are constrained to the caller’s permitted FHIR compartments (patient, organization, and profile scopes), then further filtered by resource-type criteria and field-level read/write constraints; unauthorized rows are excluded at the query layer rather than concealed in the interface. Roles — practitioner, supervisor, biller, scheduler, and portal client — resolve to distinct least-privilege AccessPolicies. Client-portal access is scoped per client and enforces guardian and couples visibility rules. Administrative and on-behalf-of access requires an admin membership and is recorded as a FHIR AuditEvent.

7. Audit Logging & Monitoring

Access and mutation events are recorded as FHIR AuditEvent resources (actor, action, target, timestamp) and retained for retrospective analysis; the append-only history model independently preserves full record version lineage. Infrastructure-layer events are captured via AWS CloudTrail and CloudWatch, with automated monitoring of scheduled and background processing.

8. Network & Edge Security

- All infrastructure operates within an isolated Virtual Private Cloud; security groups follow least privilege, restricting traffic to required ports and approved sources.
- Ingress transits Amazon CloudFront with AWS Shield DDoS protection and AWS WAF (managed rule sets) on the application, front-end, and storage distributions.
- Public object access is disabled at the bucket level; all external connections terminate over TLS at the edge.

9. Change Management & Vulnerability Management

- Changes flow through version control with peer review, automated test suites, and pre-deployment verification; separate non-production and production environments are maintained.
- Infrastructure is defined as code and subject to the same review path.
- Automated dependency vulnerability alerting is enabled on all source repositories; findings are triaged and remediated by severity.
- Recurring internal adversarial security audits are conducted against AccessPolicy enforcement and server-side authorization boundaries.

10. Artificial Intelligence Processing

AI-assisted documentation is optional and configured per practice; session recording requires client consent in the workflow. Audio is transcribed by Deepgram (primary) and Groq (fallback); clinical note drafting is performed by Anthropic — each operating under an executed Business Associate Agreement. Use of PHI for AI model training is contractually prohibited (BAA § 4.5). Session audio is processed for transcription and then deleted; recordings are not stored as durable records. Transcript retention is practice-configurable, with automated daily purge of expired transcripts (7-day minimum). No AI-generated content is committed to the record without clinician review and electronic signature.

11. HIPAA Safeguards Summary

45 CFR REFERENCE	SAFEGUARD	IMPLEMENTATION
164.312(a)(1)	Access control	Per-membership AccessPolicy; compartment scoping; least-privilege roles
164.312(b)	Audit controls	FHIR AuditEvent logging; append-only version history; CloudTrail

45 CFR REFERENCE	SAFEGUARD	IMPLEMENTATION
164.312(c)(1)	Integrity	Immutable per-resource versioning; managed change control
164.312(d)	Person/entity authentication	bcrypt credentials; signed JWT sessions; TOTP MFA
164.312(e)(1)	Transmission security	TLS 1.2+ in transit; TLSv1.2_2021 edge minimum
164.312(a)(2)(iv)	Encryption at rest	AES-256 (Aurora + S3) under AWS KMS
164.308(a)(1)	Security management / risk analysis	Documented Security Risk Analysis, reviewed ongoing
164.308(b)(1)	Business associate contracts	BAA register; executed BAAs with all PHI subprocessors
164.308(a)(6) / HITECH	Incident & breach response	Notification without unreasonable delay per HIPAA/HITECH/BAA
164.310	Physical safeguards	Inherited from AWS data centers (subservice organization)

12. Subprocessors

VENDOR	FUNCTION	PHI	LOCATION
Amazon Web Services	Compute, database, storage, KMS, CDN/WAF, email	Under AWS BAA	US
Deepgram	Speech-to-text transcription (primary)	Executed BAA	US
Groq	Speech-to-text transcription (fallback)	Executed BAA	US
Anthropic	LLM clinical-note drafting; no-training terms	Executed BAA	US
Stedi	X12 EDI clearinghouse (837P/270/276/835)	Executed BAA	US
Stripe	Payment processing (per-practice account)	No PHI by design	US

13. Data Portability & Vendor Independence

Records are maintained in the FHIR R4 open standard; no proprietary record schema is used. Complete structured exports are available on request, including upon termination. Payment processing is performed through each practice's own Stripe account, which remains practice property; cardholder data is transmitted directly to Stripe and is not stored on Practice Harbor systems.

14. Contact

Security documentation requests, questionnaire responses, and vulnerability reports: **albert@practiceharbor.com**. Good-faith security research will not be subject to legal action. This document is updated as the system and its controls evolve; the canonical, current version is published at practiceharbor.com/trust.

15. Scope and Limitations

This Security Overview is a self-attestation prepared by Practice Harbor management. It has not been examined or attested to by an independent auditor and does not constitute a SOC 2, ISO 27001, or HITRUST report. Statements describe the design of controls as of the effective date; they do not represent an opinion on operating effectiveness over a period of time.

HIPAA establishes no governmental certification scheme for software, and Practice Harbor makes no claim of HIPAA certification. Compliance is demonstrated through the administrative, physical, and technical safeguards enumerated in Sections 3–11 of this document.

Physical and environmental controls are inherited from Amazon Web Services as a subservice organization and are outside the boundary of this description. Certain controls assume corresponding actions by customer practices, including administration of their own user access, enforcement of multi-factor authentication, and management of their own Stripe account.

This document is provided for informational purposes and does not constitute a contract. Controlling legal terms are set by the Business Associate Agreement (practiceharbor.com/baa), the Terms of Service, and the Privacy Notice. The current version of this document is published at practiceharbor.com/trust.

© 2026 Somatopia, LLC dba Practice Harbor. Self-attestation; not an independent audit report. Document version 1.0 · August 2026.