

EnWella Security One-Pager

Procurement-ready summary. For full controls, see `DATA SECURITY POLICY.md`.

At a glance

Topic	Posture
HIPAA	Live. Privacy Rule + Security Rule.
Business Associate Agreement	Available; signed for every customer at account creation.
Cloud provider	Major US public cloud, HIPAA-eligible services under an executed BAA (SOC 2 Type II + ISO 27001). Named on request.
Encryption (transit)	TLS 1.3 preferred, TLS 1.2 minimum. HSTS pinned. No unencrypted HTTP.
Encryption (rest)	AES-256 across database, object storage, and backups. Managed cloud KMS. CMEK on request.
Authentication	Unique user identity. Minimum 8-char complex password, bcrypt (cost 12). MFA available for all users; passkey (WebAuthn) required for EnWella admin consoles. Lockout after 10 failed attempts. 24h inactivity timeout.
Authorization	Pundit role-based access. 13 granular role flags. Minimum-necessary enforced per resource, server-side.
Audit logging	Every PHI read + write logged with actor, timestamp, and request context. 7-year retention.
AI	Runs on a HIPAA-eligible, BAA-covered enterprise AI service inside our cloud boundary. No PHI used to train any model. Output is a provider-reviewed draft.
Data residency	United States only. No offshore processing or support.
Breach notification	Customer notified without unreasonable delay and no later than 30 calendar days after discovery — half the HIPAA maximum. Shorter periods available by negotiated amendment.

Hosting

- **Region:** United States only (specific region on request).
- **Database:** Managed PostgreSQL, private IP, deletion-protected, with point-in-time recovery and automated daily backups (7-day backup retention).
- **Object storage:** Managed cloud object storage with bucket-level IAM and encryption at rest.
- **Secrets:** Managed secret store with versioned, audit-logged access. No secrets in source.
- **Recovery objectives:** RTO 24h / RPO 4h.

Sub-processors

Current as of the date below. EnWella notifies customers **30 days before** adding any new sub-processor that handles ePHI, and a customer may terminate without penalty if it objects.

Function	Handles PHI	BAA
Cloud infrastructure (hosting, database, object storage, KMS)	Yes	Yes
Enterprise AI (transcription, draft documentation, assistant)	Yes	Yes
Video conferencing + calendaring (telehealth visits)	Yes	Yes
Telecommunications (voice + SMS for front desk and reminders)	Yes	Yes
Electronic signature — self-hosted inside EnWella infrastructure	Yes	N/A — not a third party
Clinical fax	Yes	Yes
Claims clearinghouse (eligibility + 837P submission)	Yes	Yes
Electronic prescribing	Yes	Yes
Transactional email (no PHI in subject lines)	Limited	Yes
Payment processing	No — PCI scope only	N/A — PCI DSS
Mobile push delivery (envelopes only)	No	N/A
Error + reliability monitoring (PHI excluded from payloads)	No	N/A
DNS for customer custom domains	No	N/A

The named vendor behind each function is provided on request under NDA or under an executed BAA. We describe sub-processors by function here so that a vendor change does not require re-papering every customer agreement.

Application security

- Static application security testing on every push (`brakeman`).
- Dependency scanning + automated patches for high/critical CVEs.
- Code review required for every production change.
- Production environment isolated from staging; per-environment credentials.

Incident response

- Named **Security Officer + Privacy Officer**.
- Documented incident-response runbook; severity-based escalation.
- 24/7 alerting on key surfaces.
- Breach of Unsecured PHI reported to the affected customer **without unreasonable delay and no**

later than 30 calendar days after discovery — half the maximum permitted by 45 C.F.R. § 164.410. In practice we notify as soon as scope is established; shorter contractual periods are available by negotiated amendment.

Workforce

- HIPAA training within 30 days of hire and annually thereafter.
- Confidentiality + data-handling agreements signed before access.
- Least-privilege access provisioning; revoked immediately on termination.

Customer rights

- Export your data on request (CSV bundle).
- Delete your data on contract termination per the BAA retention schedule.
- Read-only audit-log export on request.
- BAA available before any production data lands in EnWella.

Contact

- **Security Officer:** support@enwella.com
- **Privacy Officer:** support@enwella.com
- **Status page:** <https://enwella.com/status>
- **Changelog:** <https://enwella.com/changelog>

Document generated from `docs/legal/SECURITYONEPAGER.md`. Last updated August 13, 2026.
