HIPAA Compliance

Checklist & Implementation Guidelines

WellHub Multi-Tenant SaaS · Version 2.1.0

Generated: 11/17/2026, 9:22:00 PM
Document date: 2026-11-06

Readiness score

55%

Complete: 14 · Partial: 4 · Pending: 6 · Not started: 5 · Total: 29

Administrative Safeguards: 2/8 complete
Physical Safeguards: 1/3 complete
Technical Safeguards: 10/14 complete
Organizational Requirements: 1/4 complete

Executive summary

WellHub is a multi-tenant healthcare SaaS platform. HIPAA compliance is a shared responsibility: the platform (Business Associate) implements technical and organizational safeguards; each tenant (Covered Entity) completes administrative requirements, signs a BAA, and trains workforce members. Production PHI relies on HIPAA-eligible services from subprocessors such as MongoDB Atlas and Google Cloud (Firebase Auth and related Covered Services); maintain executed BAAs with those vendors for your production accounts. This document maps the HIPAA Security Rule to WellHub capabilities as of 2026-11-06.

1. Multi-tenant data isolation

- All PHI is scoped by organizationId at the database and API layer.
- Cross-tenant access is blocked; API guards enforce org boundaries on every request.
- Platform administrators see metadata only (counts, usage events) — not patient row data by default.
- Support access requires super_admin role, is time-limited (8 hours), and is audit-logged.

2. Tenant provisioning & licensing

- Platform provisions tenants with unique ID, slug, and one-time provision secret.
- Tenants activate via POST /api/tenant/activate before production use.
- Licensed modules (AWV, compliance, API, AI Assist) are assigned per plan or explicitly.
- BAA must be signed before PHI access; subscription must be active.

3. Usage-based billing without PHI exposure

- Billable events (logins, claims, reports, AI inferences) use hashed resource IDs only.
- Usage ledger (usage_events) stores event type, quantity, and metadata — never clinical content.
- Stripe metered billing sync runs via scheduled job with CRON_SECRET.
- Tenants can view their own usage at Settings ⁉ Billing.

4. Embed & custom domain delivery

- Tenants may embed WellHub in ERP/website via iframe with origin allowlist.
- Short-lived embed JWT tokens (15 min) bind session to allowed origin.
- Native subdomain: {slug}.wellhubscreen.com when PLATFORM_DOMAIN is configured.
- CSP frame-ancestors relaxed only on /embed routes.

5. API & insurance billing

- Professional+ plans: API keys (whb_…) for claims validate/submit and report generation.

- Claims validated before submit; transactions tracked in bridge_transactions.
- All bridge actions logged to audit_logs and usage_events.

6. AI Assist sandbox (testing mode)

- AI Assist is licensed separately; enabled by platform provider for client evaluation.
- Sandbox accepts synthetic demo patients only (demo-* IDs). Real patient records are rejected.
- Platform manages Azure OpenAI or OpenAI via environment variables — keys never stored in database.
- AI inference telemetry is metadata-only (mode, token count, provider) for platform billing.
- Production PHI mode requires separate BAA amendment, tenant opt-in, and risk assessment.

7. Tenant onboarding checklist (practice actions)

- Designate a HIPAA Security Officer in Compliance Center.
- Sign the Business Associate Agreement electronically.
- Complete workforce HIPAA training; attest annually in Compliance Center.
- Conduct Security Risk Assessment (SRA) and document remediation plan.
- Review user access quarterly; remove terminated staff promptly.
- Enable MFA for all users under Settings!' Security.
- Document incident response and breach notification procedures.

8. Ongoing compliance (annual & event-driven)

- Re-evaluate HIPAA compliance annually and after operational changes.
- Verify executed BAAs with all subprocessors (MongoDB Atlas, Google Cloud/Firebase, Stripe, Resend; Azure OpenAI or OpenAI if AI Assist uses PHI).
- Export audit logs periodically from Compliance Center.
- Download updated compliance packet after BAA signing or major platform changes.
- Report suspected breaches to WellHub within 24 hours; HHS notification within 60 days if required.

9. Platform technical controls (WellHub)

- AES-256-GCM field-level encryption for PHI at rest.
- HTTPS/TLS, HSTS, and Content-Security-Policy for data in transit.
- Firebase authentication + server-side session store with timeout.
- TOTP MFA available; RBAC (admin, provider, medical assistant).
- audit_logs collection with 7-year retention target.

- compliance_alerts and compliance_tasks for continuous monitoring.

HIPAA Security Rule checklist

Administrative Safeguards

Security Officer designated [Not started]

§164.308(a)(2) · Practice
Assign a HIPAA Security Officer responsible for developing and implementing security policies.

Workforce HIPAA training [Not started]

§164.308(a)(5) · Practice
Train all staff on privacy, security, and breach reporting before PHI access and at least annually.

Access management & authorization [Complete]

§164.308(a)(3-4) · WellHub
Role-based access (admin, provider, medical assistant). User approval required before login. Team invites org-scoped.

Periodic access review [Action needed]

§164.308(a)(3)(ii)(C) · Practice
Review user access quarterly. Remove terminated staff promptly via Admin!' Users.

Security incident procedures [Action needed]

§164.308(a)(6) · Practice
Document breach detection, containment, and notification procedures (HHS within 60 days; individuals without unreasonable delay).

Contingency plan & data backup [Partial]

§164.308(a)(7) · Shared
MongoDB Atlas provides automated backups. Practice should document disaster recovery and emergency mode operations.

Periodic technical & non-technical evaluation [Action needed]

§164.308(a)(8) · Practice
Re-evaluate HIPAA compliance at least annually and after environmental or operational changes.

Platform support access controls [Complete]

§164.308(a)(3)(ii)(A) · WellHub
Super-admin support access is time-limited (8 hours), cookie-scoped, and logged as support_access audit events — no standing PHI access.

Physical Safeguards

Facility access controls [Complete]

§164.310(a) · Shared
PHI is hosted on SOC 2 / HIPAA-eligible cloud infrastructure (MongoDB Atlas, Google Firebase). Verify BAAs with cloud providers.

Workstation use & security [Action needed]

§164.310(b) · Practice
Policies for devices accessing PHI: screen lock, no shared logins, encrypted disks, no PHI on personal devices.

Device & media controls [Action needed]

§164.310(d) · Practice
Secure disposal of hardware/media containing PHI. Do not export PHI to unencrypted USB or email.

Technical Safeguards

Unique user identification [Complete]

§164.312(a)(1) · WellHub
Each user has a unique Firebase account. Sessions bound to user ID and organization.

Multi-factor authentication (MFA) [Partial]

§164.312(d) · Shared
TOTP-based MFA with backup codes available. Enable MFA for all users under Settings⁉ Secur

Automatic logoff / session timeout [Complete]

§164.312(a)(2)(iii) · WellHub
Sessions expire after 1 hour of inactivity. JWT validated against server-side session store.

Encryption at rest (PHI fields) [Complete]

§164.312(a)(2)(iv) · WellHub
Patient demographics and clinical fields encrypted with AES-256-GCM. MongoDB Atlas encryption at rest.

Encryption in transit [Complete]

§164.312(e)(1) · WellHub
All traffic over HTTPS/TLS. HSTS and strict Content-Security-Policy headers enforced.

Audit controls & logging [Complete]

§164.312(b) · WellHub
Patient access, modifications, auth events, and exports logged to audit_logs with 7-year retention target.

Integrity controls [Complete]

§164.312(c)(1) · WellHub
Field-level encryption and authenticated encryption (GCM) protect PHI from unauthorized alteration.

Multi-tenant data isolation [Complete]

§164.308(a)(4) · WellHub
All patient, visit, and template data scoped by organizationId. Cross-tenant access blocked at API layer.

Minimum necessary standard [Partial]

§164.502(b) · Shared
Role-based permissions limit data access. Only assign admin role to users who require it.

Usage billing without PHI in ledger [Complete]

§164.502(b) · WellHub
Billable usage events (logins, claims, reports, AI inferences) store hashed resource IDs and metadata only — never clinical content.

Platform admin metadata-only access [Complete]

§164.502(b), §164.314(a) · WellHub
Platform administrators view tenant counts and usage aggregates only. Patient row data is not exposed in platform analytics.

AI Assist sandbox (synthetic patients only) [Complete]

§164.308(b)(1), §164.502(e) · Shared
AI Assist is optional. When not licensed, no patient data is sent to AI providers.

Embed & iframe origin allowlist [Partial]

§164.312(e)(1) · Shared
Embedded dashboards use short-lived JWT tokens bound to tenant-configured allowed origins. Configure allowlist before production embed.

API & claims audit trail [Not started]

§164.312(b) · Shared
Insurance billing API (Professional+ plans) validates claims before submit, logs bridge_transactions, and records usage events for billing.

Organizational Requirements

Business Associate Agreement (BAA) [Not started]

§164.502(e), §164.504(e) · Practice
Execute a BAA with WellHub before creating, storing, or transmitting PHI. Required for all covered entities.

Subprocessor / vendor inventory [Complete]

§164.502(e)(1)(ii) · Shared
Maintain a list of vendors that handle PHI (MongoDB Atlas, Firebase, Resend, Stripe, Azure OpenAI when AI Assist is enabled). Available in the compliance packet and HIPAA PDF.

Security risk assessment (SRA) [Action needed]

§164.308(a)(1)(ii)(A) · Practice
Conduct an annual risk analysis of PHI threats and vulnerabilities. Document findings and remediation plan.

Tenant activation & BAA before production PHI [Not started]

§164.308(b)(1) · Practice
Complete tenant activation with provision secret. BAA must be signed before creating or accessing live patient records.

Subprocessor inventory

- MongoDB Atlas — Primary database — PHI storage (encryption at rest), backups
  US region (Atlas cluster) · BAA: Eligible / available — MongoDB Atlas HIPAA-eligible deployment + MongoDB Atlas Business Associate Addendum
- Google Cloud (Firebase / Identity) — Authentication (Firebase Auth), Google Cloud–covered services as configured
  US (Firebase/Google Cloud project region) · BAA: Eligible / available — Google Cloud BAA covering Covered Services (includes Firebase when in scope for your project)
- Google Cloud Storage — Optional file/document storage when enabled
  US bucket (recommended for PHI) · BAA: Eligible / available — Google Cloud BAA (Cloud Storage as a Covered Service)
- Resend — Transactional email (invites, notifications — minimize PHI in email body)
  US · BAA: Eligible / available — Resend HIPAA BAA upon request / HIPAA offering (confirm current terms before production)
- Stripe — SaaS subscription & usage-based billing (metadata; no clinical content)
  US · BAA: Eligible / available — Stripe HIPAA Business Associate Agreement (for eligible services)
- Microsoft Azure OpenAI — Optional AI Assist — inference when platform uses Azure OpenAI
  US Azure region · BAA: Eligible / available — Microsoft HIPAA BAA for Azure services in scope (include Azure OpenAI if used with PHI)

• OpenAI — Optional AI Assist — inference when platform uses OpenAI API
US (API configuration–dependent) · BAA: Eligible / available — OpenAI Business Associate Agreement for eligible API use (required before production PHI)

This document is for compliance guidance only and does not constitute legal advice. Consult qualified counsel for HIPAA compliance determinations. WellHub checklist scores reflect automated platform readiness plus documented tenant actions — not a certification of compliance.