



FOR TEAMS THAT TOUCH PHI

HIPAA for teams that ship with AI.

If you handle protected health information for a covered entity, you are a business associate and HIPAA applies to you, your cloud, your LLM provider and your support tools. Here is what the hospital's security team will ask, and how to already have the answer.

WHAT THE HOSPITAL WILL ASK

- **Where does PHI live and flow?** Every store, every queue, every prompt.
- **Is there a BAA with every sub-processor that can see it?** Cloud, database, LLM, analytics, support desk, email.
- **Encrypted at rest and in transit, verified?** Not assumed.
- **Minimum-necessary access, logged?** Who saw what, when, tamper-evident.
- **Breach plan?** Written, rehearsed, 60-day clock understood.
- **What can your AI do with our data?** Training use, retention, human oversight, kill switch.

THE BAA MATRIX

LAYER	NEEDS A BAA WHEN
Cloud and database	PHI is stored or processed there (AWS, GCP, Azure, Supabase)
LLM provider	PHI appears in prompts, context or fine-tuning
Analytics and logging	Identifiers or free text reach the vendor
Support and email	Patients or clinicians can write PHI into a ticket
Contractors	Anyone with production access

HOW KOLLGUARD GETS YOU THERE continuous, not the week before the audit

1

Scan the real stack

Repos, cloud and Postgres graded against the HIPAA Security Rule safeguards and SOC 2 criteria. Encryption, access, logging, secrets, RLS, verified from configuration.

2

Fix as pull requests

Sentinel turns findings into reviewable PRs. AI-drafted remediations, a human approves, evidence records itself.

3

Track every BAA

One register of BAAs, DPAs and MSAs with the signed document attached, linked to the vendor and the AI system it covers, reminders before expiry.

4

Answer and prove

Paste the hospital's questionnaire; KGAI drafts every answer from your real posture with a policy citation and confidence. Publish a Trust Center and the next one gets shorter.

WEEK ONE

Posture scan and BAA gap list

Connect GitHub and cloud, import vendors from CSV, see which safeguards already pass and which sub-processors have no BAA.

MONTH ONE

Findings closed, evidence flowing

Open PRs merged, policies drafted and approved, AI inventory recorded, Trust Center live.

AUDIT

An export, not a project

Evidence package covering the period; a vetted independent auditor from the marketplace when you want the real opinion.

START FREE

Scan the repo that handles PHI

Findings mapped to HIPAA and SOC 2 controls in minutes.

kollguard.com/free/repo-scan

FREE GUIDE

HIPAA for AI startups, with the BAA matrix

Plain-English, no signup.

kollguard.com/guides/hipaa-for-ai-startups

TALK TO US

18 years inside hospital IT

Epic programs at Cedars-Sinai, Cleveland Clinic, Sutter and Stanford. We know what the reviewer wants.

raj@kollguard.com

ON STAGE IN 2026 Where KollGuard has pitched, exhibited and sponsored this year · kollguard.com/spotlight

JUL 18–19

AGI Summit

Startup track · customer exchange

JUL 30 – AUG 1

Stanford AI Summit

Exhibitor · main-stage pitch

AUG 26–27

Step SF

Spotlight Startup · pitch competition

SEP 17–18

ISACA Sacramento 2026

Platinum sponsor · speaker session