BAA readiness checklist for your vendor stack

For EHR integration, custom EHR and healthcare data teams. Checked November 13, 2026.

Nirmitee.io

1. Every tool that can reach PHI

Tool	How PHI reaches it	Ready when
☐ **Cloud hosting**	Databases, storage, queues, backups	Use only services on the provider's covered list (AWS HIPAA Eligible Services, Azure in-scope services, Google covered products).
☐ **AI and LLM APIs**	Prompts, files, outputs, retention	BAA accepted for the right organization; only eligible features; retention settings per vendor docs.
☐ **SMS and voice**	Appointment texts, call recordings	BAA or addendum signed before messages carry PHI.
☐ **Email**	Patient emails, attachments	BAA on the plan you use, or keep PHI out of email.
☐ **CRM and marketing**	Patient lists, forms, notes	BAA on a plan that offers one, or no patient data in the CRM.
☐ **Product analytics and pixels**	Events, URLs, session replays	Strip PHI from events, or a BAA. No tracking pixels on logged-in pages without one.
☐ **Logs and error tracking**	Payloads, stack traces	Log IDs and error codes, not payloads. BAA if PHI can still reach the tool.
☐ **Support desk**	Screenshots, chart details	Separate channel for PHI; BAA if tickets can hold it.
☐ **Data warehouse and lake**	Landing buckets, failed rows, backups	BAA with the platform and cloud; trace one failed record end to end.

Check the plan tier. Many vendors offer a BAA only on paid or enterprise plans, and only for listed services.

2. Your BAA includes the required terms (45 CFR 164.504(e))

- ☐ Permitted uses of PHI
- ☐ No other use or disclosure
- ☐ Security Rule safeguards
- ☐ Report incidents and breaches
- ☐ Subcontractor flow-down
- ☐ Patient access and amendment
- ☐ Privacy Rule duties you take on
- ☐ HHS access to records
- ☐ Return or destroy PHI
- ☐ Termination for material breach

3. Before the first real record

- ☐ BAA signed with the customer
- ☐ Subcontractor BAAs signed
- ☐ HIPAA risk analysis written
- ☐ Named engineers and locations agreed
- ☐ Breach notice deadline your team can meet
- ☐ Offboarding plan for every copy

Nirmitee signs BAAs for EHR integration, custom EHR development and healthcare data engineering when the agreed work requires us to handle PHI. Book a free 30-minute PHI data-flow review: cal.com/nirmitee.io/30min

Not legal advice. Sources: 45 CFR 160.103, 164.502(e), 164.504(e), 164.410; HHS guidance; vendor HIPAA pages.

nirmitee.io/blog/hipaa-business-associate-agreement-baa-software-vendors/