FILLABLE CHECKLIST · VENDORS · PHI

Before patient data touches a vendor, *run this list.*

A fillable vetting checklist for any AI vendor that will touch PHI: whether a BAA is required, what the BAA must contain, and the questions the contract won't answer for you.

PREPARED FOR YOUR LEGAL COUNSEL
This is a template prepared for you to take to your own attorney. Have your legal counsel review and adapt it for your state and your practice before you adopt it, use it in your practice, or put anything from it in front of patients. Laws vary by state; this is not a final legal instrument and is not legal advice.

WHAT THIS IS
A four-part checklist built from HHS's business associate guidance and the required BAA elements at 45 CFR 164.504(e): does this vendor need a BAA, does the offered BAA contain the required elements, what to ask beyond the BAA, and red flags requiring resolution before approval.

HOW TO USE IT
Complete one copy per vendor, before signing and before any PHI flows. Keep the completed checklist with the executed BAA. Bring unresolved items to your attorney; do not resolve them by hoping.

Vendor / tool: _____

Completed by: _____

Date: _____

Part A. Does this vendor need a BAA?

☐ The tool will **create** PHI on our behalf (e.g., drafts clinical notes from encounter audio).

☐ The tool will **receive** PHI from us (uploads, integrations, dictation, message content).

☐ The tool will **maintain** PHI (stores recordings, transcripts, drafts, embeddings, logs).

☐ The tool will **transmit** PHI (sends data to its cloud, subcontractors, or the EHR).

If any box is checked and the vendor performs that function or service on the practice's behalf, the vendor is generally a business associate and a BAA is required before use; confirm unusual arrangements, such as treatment disclosures, workforce relationships, or conduit claims, with counsel (45 CFR 160.103; HHS Business Associates guidance). No box checked? Document why, and re-check if the use changes.

Scope note: this checklist covers federal HIPAA. State privacy, medical-records, and breach-notification laws may impose stricter vendor requirements; confirm your state's rules with counsel.

Part B. The offered BAA contains the required elements (45 CFR 164.504(e))

☐ States the permitted and required uses and disclosures of PHI by the vendor.

☐ Prohibits use or disclosure beyond the contract or as required by law.

☐ Requires appropriate safeguards, including Security Rule compliance for ePHI.

☐ Requires the vendor to report unauthorized uses and disclosures, including breaches of unsecured PHI.

☐ Makes PHI available for patient access, amendment, and accounting of disclosures.

☐ Requires compliance with Privacy Rule obligations the vendor performs for us.

☐ Makes the vendor's books and records available to HHS.

☐ Requires return or destruction of PHI at termination, if feasible.

☐ Flows the same restrictions down to the vendor's subcontractors.

☐ Authorizes termination for material violation.

Part C. Questions the BAA alone will not answer

☐ **Training:** Is our data used to train or improve the vendor's models? Where is that stated in writing, and can we opt out?

☐ **De-identification rights:** Does the contract let the vendor de-identify our PHI and keep using it? (HHS model language treats this as an optional provision. It is a business decision, not a default. Strike it or price it.)

☐ **Retention:** How long are recordings, transcripts, and drafts kept? Can we set retention to the minimum our workflow needs?

☐ **Location and subcontractors:** Where is data stored and processed, and which subcontractors touch it? Are they under equivalent agreements?

☐ **Breach clock:** How quickly does the vendor notify us of a breach, in hours or days, in writing?

☐ **Exit:** At termination, how do we export our data, and what proof of destruction do we receive?

Part D. Red flags requiring resolution before approval

- The vendor will not sign a BAA but says the product is "HIPAA compliant." Compliance claims without a BAA transfer nothing.
- The product permits or technically processes PHI on a tier for which the vendor will not execute a BAA.
- Consumer-grade terms of service govern clinical data.
- The vendor cannot say, in writing, whether your data trains their models.
- Nobody at the vendor can name their subcontractors that touch PHI.
- Patient data is stored or processed outside the United States, and the vendor cannot document adequate safeguards or contractual protection for it.

Disposition

Decision (approve / reject / conditions):

_____

BAA signed date: _____

Next review date: _____

SOURCES · CHECK OUR WORK

HHS. Business Associates. hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates

HHS. Sample Business Associate Agreement Provisions. hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions

HHS/OCR. Guidance on Risk Analysis. hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis