BAA Vendor Checklist

Run this against every vendor on your PHI map: classify, verify the ten required clauses, check the contract's real coverage. One row of the worksheet per vendor.

1 · DOES THE VENDOR NEED A BAA? — 45 CFR §160.103

- ☐ Creates, receives, maintains, or transmits PHI → business associate: signed BAA before PHI flows
- ☐ Transmission-only, storage merely transient → conduit (narrow; persistent storage never qualifies)
- ☐ Payment processing by a financial institution → §1179 exempt, for the payment activity only
- ☐ Encrypted, vendor holds no key → still a business associate (HHS cloud-computing guidance)

2 · THE TEN REQUIRED CLAUSES — 45 CFR §164.504(e)(2)

- ☐ Permitted and required uses and disclosures established up front
- ☐ No use or disclosure beyond the contract or the law
- ☐ Safeguards + Security Rule compliance for ePHI
- ☐ Breach and impermissible-use reports to you (§164.410)
- ☐ Subcontractor flow-down — same restrictions and conditions
- ☐ Patient access support (§164.524)
- ☐ Amendment support (§164.526)
- ☐ Data for an accounting of disclosures (§164.528)
- ☐ Internal practices, books, records open to HHS
- ☐ Return or destroy PHI at termination + termination right for material breach

3 · FIVE CHECKS BEFORE YOU RELY ON IT

- ☐ Scope: the exact product AND plan you pay for is covered in writing
- ☐ Configuration: your settings match the vendor's HIPAA reference architecture
- ☐ Breach window: vendor→you days and you→customer days, both in the runbook
- ☐ Termination: deletion timeline, export format, destruction certificate
- ☐ AI vendors: zero-data-retention mode and exact endpoints covered in writing

4 · RED FLAGS — STOP AND FIX

- ☐ Free or consumer tier carrying PHI — BAAs almost never cover them
- ☐ "We're just a conduit" from anything that stores messages, files, or recordings
- ☐ De-identify-and-retain rights granted by default — make it a deliberate yes/no
- ☐ Plan downgrade or new vendor sub-processor since the BAA was signed
- ☐ BAA drafted and emailed but never countersigned — absence cost CCDH $31,000

PER-VENDOR WORKSHEET — one line per vendor, file with your risk analysis

Vendor _____ · PHI it touches _____ · Classification: BA / conduit / §1179 / workforce / no-PHI · BAA signed (date) _____ · Product + plan covered ✓/✗ · Breach window _____ days · Sub-processors verified ✓/✗ · Configuration matches vendor HIPAA guidance ✓/✗