Secure Nomad

Enterprise security, practice-sized.

FREE ARTIFACT 2 OF 3 · THE BAA ADEQUACY TEMPLATE

The BAA Adequacy Template

Four questions · read the agreement against the product as it exists today

Most BAAs predate the AI features they now govern. *They are silent on what matters.*

Read the agreement against the product as it exists today, not as it existed at signature. Four questions, that is the whole review. A silent answer is a contractual gap, fixed with a letter and an amendment, not a product. One sheet per AI-positive vendor; full read on your three highest-exposure agreements.

Vendor	Agreement / signed	Governs (product, features)	Reviewed by / date

The four delta questions

§164.308(b)(1) · §164.314(a)(2)(i) · §164.504(e)(2) · §164.514(b)

	QUESTION	AGREEMENT SAYS (CLAUSE, PAGE)	VERDICT	GAP
1	Is PHI from our account used to **train or improve models**?		☐ Prohibits ☐ Permits ☐ Permits, opt-out ☐ Silent	
2	Did the AI feature introduce **new subprocessors**, and are they named?		☐ Named, flow-down ☐ Generic list ☐ Silent	
3	Did **data retention** change when the feature shipped?		☐ Stated, unchanged ☐ Stated, changed ☐ Silent	
4	Do the vendor's **de-identification** claims survive scrutiny?		☐ Safe Harbor documented ☐ Expert determination ☐ Marketing language only ☐ Silent	

Coverage check

- ☐ The agreement names the AI feature or the product version containing it
- ☐ It covers the media the feature ingests (audio, images, text)
- ☐ It addresses subprocessor breach notification
- ☐ It addresses return or destruction of inputs at termination

Adequacy verdict

- ☐ **Adequate** as written for today's data flows
- ☐ **Amend.** Gaps above are addressable. Send the amendment request.
- ☐ **Inadequate, no path.** Vendor refuses amendment or written answers. This is Gate 1 of the decision tree.

Why "current" is the word that matters at renewal.

The questionnaire asks whether every vendor touching PHI has a signed, **current** business associate agreement. When the data flows changed and the contract did not, current is exactly the word you cannot certify. Send the one-sentence question: *Is PHI from our account used to train, fine-tune, or improve any model, and which subprocessors receive it, under what agreement?* The written answer goes in the file. So does the written refusal.

Three rules

- **Silent is a finding, not a failure.** Write "silent", cite the absence, move to the letter.
- **"De-identified" in a sales paragraph is neither Safe Harbor nor expert determination.** Ask for the documentation; file the answer or its absence.
- **The written no goes in the file.** Diligence is proven by the ask, not the outcome.

Ricky Martin

CISSP, CCSP, CISM · twenty years in enterprise cybersecurity, now working only with independent practices.

securenomad.ai/ISACA

ISACA New England 50th AGM · September 10, 2026

Free to use and share. No forms, no gate. Not legal advice.