Secure Nomad

Enterprise security, practice-sized.

FREE ARTIFACT 1 OF 3 · THE 12-QUESTION AI VENDOR CHECKLIST

The 12-Question AI Vendor Checklist

Send to every vendor that touches PHI · waypoints one to three · mapped to the Security Rule

Your vendor list did not change. *Your vendors did.*

The products you license shipped AI since anyone last looked, in a software update, not a purchase order, and the register still says green. You do not have to do the research yourself. Send these twelve questions to every vendor that touches protected health information; their answers populate your inventory. A vendor who will not answer in writing has also told you something worth writing down.

Vendor	Product	Our last review date	Sent / answered

Waypoint 1 · AI delta inventory

45 CFR §164.308(a)(1)(ii)(A) risk analysis · §164.308(b)(1) business associate contracts

	QUESTION	VENDOR'S WRITTEN ANSWER
1	Since our last review on the date above, which AI or machine learning features have been added to the product we license? List each with its release date.	☐ Answered ☐ Cannot say
2	Which of those features are currently enabled for our account, and who enabled them: vendor default, our administrator, or an individual user?	☐ Answered ☐ Cannot say
3	For each feature, does it process, store, or transmit PHI from our account? Answer yes, no, or unknown per feature.	☐ Answered ☐ Cannot say
4	Can individual clinicians or end users enable AI features without administrator action? If yes, where in the admin console can we see which users have done so?	☐ Answered ☐ Cannot say

Waypoint 2 · BAA delta review

§164.308(b) · §164.314(a)(2)(i) · §164.502(e) · §164.504(e)

5	Is PHI from our account used to train, fine-tune, evaluate, or otherwise improve any model? If yes, under which term of our agreement, and is there an opt-out?	☐ Answered ☐ Cannot say
6	Which subprocessors, including any model or inference providers, receive PHI in connection with the AI features, and under what agreement with you?	☐ Answered ☐ Cannot say
7	Did data retention change when the AI feature shipped? State the retention period for inputs, outputs, and intermediate artifacts such as audio, transcripts, embeddings, and prompts.	☐ Answered ☐ Cannot say
8	Where you rely on de-identification, is it Safe Harbor (all eighteen identifiers removed, §164.514(b)(2)) or expert determination (§164.514(b)(1))? Provide the documentation.	☐ Answered ☐ Cannot say

Waypoint 3 · Minimum necessary at the model boundary

§164.502(b) · §164.514(d) · §164.312(a)(1) access control

9	Exactly which fields, document types, and media (audio, images, free text, attachments) does each AI feature receive from our system?	☐ Answered ☐ Cannot say
10	Can we restrict that scope by field, document type, user, or location before transmission? Where is it configured, and will you confirm our configuration in writing?	☐ Answered ☐ Cannot say
11	Is data redacted, truncated, or de-identified before it leaves our environment, or only after it reaches yours?	☐ Answered ☐ Cannot say
12	Who at your company owns these answers, and will you give written notice before any material change to AI capability or subprocessors, and let us disable the feature pending review?	☐ Answered ☐ Cannot say

Monday morning: the short form

Three questions, one hour, before your renewal date

If you send nothing else, send these three sentences

1. Since our last review, has any AI or machine learning capability been added to the product we license, whether or not it is enabled?
2. Does PHI from our account touch a model, for inference or for training, and under what agreement?
3. Exactly which fields and document types does the AI feature receive from our system, and can we restrict them?

Send them on your own letterhead, with a ten-business-day reply date. The full twelve questions on page one go to any vendor whose answer is incomplete, and to any vendor with an AI feature you already know is enabled.

Reading the answers

WHAT CAME BACK	RECORD IT AS	THEN
All twelve answered in writing	Answered. Attach the reply as received.	Proceed to the BAA adequacy template and the field map.
Some answered, some "cannot say"	Partial. Each "cannot say" becomes an **unknown** in your inventory with a follow-up date.	A documented unknown with a date on it reads far better at renewal than silence.
No reply after two chases (day 10, day 20)	Silent. Dated.	A documented silence is evidence of diligence. File it.
Declines to answer in writing	Refused. Dated.	Feeds Gate 1 of the decision tree. The written no is file evidence.

Two rules that make Waypoint 1 work.

- **Include the clinical side.** Features enabled by clinicians count even when IT never turned them on. The scribe a physician enabled from the EHR marketplace is in scope, full stop.
- **Unknown is a finding, not a blank.** If nobody can say whether PHI reaches a model, the row says unknown with a follow-up date and an owner.

What the output looks like.

One page. Vendor, AI capability, date discovered, PHI exposure yes, no, or unknown. That page is the first page of your file, and the file is what answers the renewal questionnaire. Attestation is what you say. Evidence is what the file shows.

Never rewrite a vendor's answer

File it as received, then interpret it. A one-page inventory with the vendors' own words attached, dated, is something you could hand to an underwriter, a regulator, or a buyer's diligence team without flinching. That is the design goal for every page this framework produces.

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

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