

Vendor Security Risk Assessment Questionnaire Template

A Questionnaire to Send Before You Sign With Any New Vendor

SIM Technology Solutions • Healthcare IT & Compliance Guide • Updated September 2026

VENDOR RISK

Every new EHR, patient texting app, scheduling tool, or AI scribe you adopt is a new place your patients' data can live, and a signed Business Associate Agreement alone doesn't tell you how well a vendor actually protects it. This questionnaire is built to send directly to a vendor before you sign, so you get real answers in writing instead of a sales pitch.

How to use this: The pages that follow are the questionnaire itself, formatted so you can send them straight to a vendor's sales or security contact. Fill in the fields at the top, forward it along, and keep their written responses on file. If a vendor won't answer these questions clearly, that's useful information on its own.

TO BE COMPLETED BY VENDOR

Please answer each question below as completely as you can and return this document to us. If a question doesn't apply to your product, note that rather than leaving it blank.

Vendor / Company Name:

Product or Service Being Evaluated:

Completed By:

Date:

1. Data Handling & Access

Question	Vendor's Answer
What patient or practice data will this system access, store, or transmit?	
Who at your company can access our data, and how is that access controlled?	
Is our data logically or physically separated from other customers' data?	
Do you use our data, including PHI, to train AI or machine learning models?	

2. Encryption & Technical Safeguards

Question	Vendor's Answer
Is data encrypted at rest? What standard (e.g., AES-256)?	

Question	Vendor's Answer
Is data encrypted in transit? What protocol (e.g., TLS 1.2+)?	
Is multi-factor authentication available, and is it required for admin accounts?	
How often are systems patched, and is there a documented patching cadence?	

3. Business Associate Agreement & Compliance

Question	Vendor's Answer
Will you sign a HIPAA Business Associate Agreement (BAA)?	
Are you willing to flow down BAA obligations to any subcontractors you use?	
Do you maintain SOC 2, HITRUST, or another independent security certification?	
Where is our data physically hosted (state or country)?	

4. Incident Response & Breach Notification

Question	Vendor's Answer
Do you have a documented incident response plan?	

Question	Vendor's Answer
What is your contractual breach notification timeframe to us?	
Have you had a security incident or breach in the last 3 years? If so, briefly describe it.	

5. Subprocessors & Data Portability

Question	Vendor's Answer
What subprocessors or third parties will have access to our data?	
If we terminate service, how and when is our data returned or destroyed?	

FOR YOUR PRACTICE, NOT THE VENDOR

Once the vendor sends back their answers, use this page to evaluate what you got. This part is for your own file, not something you need to forward.

Red Flags to Watch For

- A vendor that hesitates or refuses to sign a BAA
- Vague or evasive answers about encryption, hosting location, or subcontractors
- No documented incident response process, or no clear breach notification timeframe
- "We've never had a breach" offered as the whole answer, with no description of how they'd detect or respond to one
- No clear answer on where data is hosted or how it's destroyed once the contract ends

Not sure how to read a vendor's answers?

SIM Technology Solutions reviews vendor questionnaires, negotiates BAAs, and vets new practice technology before you sign, so you're not the one deciphering a vague security answer alone. **Call 703-594-9226** or email info@simtsolutions.com.