HIPAA Compliance Vendor Questionnaire

HIPAA Compliance Vendor Questionnaire

This resource is meant to help guide your initial vendor evaluation. It's not a complete checklist, but a starting point to support your decision-making process.

Vendor Name: ________________________

Date of Meeting: _____________________

1. HIPAA Compliance Overview

• Why is HIPAA compliance important to your organization?

• Do you sign Business Associate Agreements (BAAs) with clients?

• What other compliance certifications does your company have?

2. Safeguards for Protecting PHI

• What specific safeguards do you use to protect PHI?

☐ Encryption (at rest and in transit)

☐ Role-based access controls

☐ Multi-factor authentication

☐ Secure data centers

☐ Regular security audits

☐ Other:___________________________________

• Have you undergone third-party HIPAA audits or certifications?

☐ Yes ☐ No

If yes, can you provide documentation or summaries?

HIPAA Compliance Vendor Questionnaire

3. Breach Detection & Notification

• How do you detect and respond to data breaches?

• Do you offer a Service Level Agreement (SLA) on response time, and if so, what is your SLA response time?

• What is your process for notifying clients within the required 60-day window?

4. Data Storage & Processing

• Where is PHI stored and processed?

• Is your data stored in a shared or private data center?

• Is all data stored in secure, U.S.-based environments?

5. Employee Training

• What HIPAA training do your employees receive?

☐ Role-specific

☐ Regularly updated

☐ Documented

☐ Other:___________________________________

6. Policies & Documentation

• Can you provide documentation of your HIPAA policies and procedures?

☐ Internal compliance policies

☐ Risk assessments

☐ Incident response plans

☐ Other:___________________________________

7. Support for Small Practices

• How do you support small practices in maintaining HIPAA compliance?

☐ Onboarding support

☐ Compliance guidance

☐ Simplified tools

☐ Other:______________________________

8. Data Retention & Termination

- What happens to our data if we stop using your service?

- Do you have a clear data retention and deletion policy?

9. Risk Assessments

- Do you conduct regular risk assessments?

- How do you update your security measures based on findings?

10. Internal Access Management

- How do you manage access to PHI within your organization?

- Who has access to our patient data and how is it monitored?

- What controls are in place to prevent unauthorized access?

11. Audit Logs & Activity Tracking

- Do you offer audit logs or activity tracking?

- Can clients access logs showing who accessed PHI and what actions were taken?

12. Subcontractor Compliance

- Do you use subcontractors?

- Are your subcontractors HIPAA compliant and covered under your BAA?

13. Client Support for Documentation

- What tools or templates do you offer to help clients with HIPAA documentation or compliance reporting?

HIPAA Compliance Vendor Questionnaire

- What level of ongoing support do you provide for compliance rule changes?