|  |
| --- |
| **AI Vendor Assessment Checklist**  10 Questions to Ask Before You Sign |

|  |
| --- |
| **HOW TO USE THIS CHECKLIST**  Complete this form for every new AI tool before deployment. A single "No" on a Critical (★) question should trigger a compliance review before proceeding. Retain completed checklists for audit documentation. |

**Vendor Information**

|  |  |
| --- | --- |
| **Vendor / Tool Name:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Product Version / Plan:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Assessed By:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Date of Assessment:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Intended Use Case:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Assessment Questions**

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Response & Notes** |
| **1**  ★ | **Does the vendor provide a Data Processing Agreement (DPA) or Business Associate Agreement (BAA)?**  Required for HIPAA-covered entities and any regulated data. Must be signed before any data is shared. | ☐ Yes ☐ No ☐ N/A  **Notes:** |
| **2**  ★ | **What data does the AI tool collect, store, or process from user inputs?**  Some tools use your inputs to train future models. This may violate client confidentiality or data sovereignty rules. | ☐ Yes ☐ No ☐ N/A  **Notes:** |
| **3** | **Where is data stored and processed geographically?**  Data residency matters for GDPR, state privacy laws, and government contractors. Confirm EU/US/other jurisdiction. | ☐ Yes ☐ No ☐ N/A  **Notes:** |
| **4**  ★ | **Does the vendor opt all accounts out of model training by default — or must you opt out manually?**  Default opt-out is the higher standard. Verify the setting exists, document how to confirm it is active. | ☐ Yes ☐ No ☐ N/A  **Notes:** |
| **5** | **What security certifications does the vendor hold?**  Look for SOC 2 Type II, ISO 27001, FedRAMP (if gov't). Ask for certificates dated within the past 12 months. | ☐ Yes ☐ No ☐ N/A  **Notes:** |
| **6** | **How long does the vendor retain user data and conversation history?**  Retention policies affect your data minimization obligations under HIPAA, GDPR, and state laws. Shorter is better. | ☐ Yes ☐ No ☐ N/A  **Notes:** |
| **7** | **Can data be deleted on request, and what is the confirmed deletion timeframe?**  Right-to-deletion requirements under GDPR, CCPA, and other laws require vendor cooperation and documentation. | ☐ Yes ☐ No ☐ N/A  **Notes:** |
| **8**  ★ | **Does the vendor have a documented incident response and breach notification process?**  You need a contractual commitment to how quickly they will notify you if your data is involved in a breach. | ☐ Yes ☐ No ☐ N/A  **Notes:** |
| **9** | **What access controls prevent vendor employees from viewing your organizational data?**  Look for role-based access controls, audit logging, least-privilege policies, and background check requirements. | ☐ Yes ☐ No ☐ N/A  **Notes:** |
| **10** | **Is there an enterprise or private deployment option that keeps all data within your environment?**  For high-sensitivity use cases, on-premise or private-cloud deployment may be required by compliance frameworks. | ☐ Yes ☐ No ☐ N/A  **Notes:** |

**Assessment Outcome**

|  |  |  |
| --- | --- | --- |
| **✓ APPROVED** | **⚠ CONDITIONAL** | **✗ NOT APPROVED** |
| All critical items passed. Add to approved tools list. | Minor gaps identified. Restrict use pending remediation steps. | Critical gaps unresolved. Do not deploy. |

|  |  |
| --- | --- |
| **Decision:** | ☐ Approved ☐ Conditional — conditions: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ☐ Not Approved |
| **Approved By:** | Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Role: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_ |