prompt

Vendor Security Checklist:

Protect your patients and practice

Safeguard PHI in the age of AI

When selecting technology partners, especially those using AI, here are some of our recommended considerations when reviewing security practices around data handling, authentication, monitoring, and any offshore labor arrangements.

Why This Matters

- **Regulatory Compliance:** Prevent HIPAA-related penalties and maintain payer agreements.
- **Patient Confidence:** Show that you prioritize privacy–strengthening patient trust and loyalty.
- **Risk Mitigation:** Secure vendors reduce downtime, data breaches, and costly remediation efforts.
- **Offshore Labor Constraints:** Some payer contracts prohibit offshore data handling and require clear documentation of vendor practices.
- **AI Data:** Ethical AI vendors will train models on data scrubbed of PHI and ensure relevancy.

Security Policies & Compliance

Risk Level: Low | Medium | High | Critical

- [ ] **Documented Security Program:** Check for formal information security policies like use of Multi-Factor Authentication (MFA) as well as regular self-audits.
- [ ] **Regulatory Frameworks:** Verify adherence to HIPAA, GDPR, and other frameworks and check if they use advanced monitoring to detect malicious traffic.
- [ ] **Incident Response:** Ask about their plan to detect, contain, and disclose breaches.
- [ ] **Security History:** Check if 24/7 monitoring is in place to catch unusual activity in real time. Investigate any past incidents and learn how they've improved prevention.

AI Vendor Review & Vetting

Risk Level: Low | Medium | High | Critical

- [ ] **Model Training & Storage:** Confirm any patient data used to train algorithms is being securely anonymized and does not violate HIPAA.
- [ ] **Bias & Transparency:** Ask how the AI vendor tests for bias and whether the output is relevant.
- [ ] **Vendor Expertise:** Ensure the AI vendor has domain experience in healthcare and HIPAA compliance, plus a record of privacy-conscious design.

AI Vendor Review & Vetting (Continued)

- [ ] **Change Management:** Clarify how they update AI models and whether such updates are reviewed for security and ethical implications.
- [ ] **Accuracy:** Ask the vendor how they ensure their AI models produce reliable results, and request clear examples demonstrating their accuracy.

Business Continuity & Disaster Recovery

Risk Level: Low | Medium | High | Critical

- [ ] **Continuity Plan (BCP):** Assess how they maintain essential services during outages or emergencies.
- [ ] **Disaster Recovery (DR):** Clarify how soon critical operations can be restored after a breach or system failure.
- [ ] **Backup Validation:** Ask about routine backup checks and the process to restore data successfully.
- [ ] **Recovery Time Objective (RTO):** Inquire about the longest acceptable downtime they anticipate for vital functions.

Subcontractors & Offshore Labor

Risk Level: Low | Medium | High | Critical

- [ ] **Third-Party Oversight:** Determine whether subcontractors play roles in data processing or software management.
- [ ] **Contractual Alignment:** Confirm that all subcontractors meet the same security standards and HIPAA obligations.
- [ ] **Offshore Considerations:** Check if offshore teams access PHI and whether this conflicts with payer agreements.
- [ ] **Notification Policy:** Ensure you are informed when the vendor engages new subcontractors.

👉 Pro Tips

- **Document Everything:** Request formal policies, recent audit reports, and AI usage disclosures.
- **Review Payer Contracts:** Some payers may require explicit consent for offshore or AI-based data handling.
- **Annual Checkups:** Incorporate vendor security reviews including AI practices into routine compliance audits.
- **Team Collaboration:** Bring in IT and compliance staff as well as your internal AI team to evaluate vendor responses thoroughly.

**Checklist provided for informational purposes only.*