**Vendor Security Agreement** ("Agreement") dated \_\_, 2025, between **[Healthcare Organization]** ("Company") and **[Vendor Name]** ("Vendor"). The parties agree as follows:

**1. Data Security and Confidentiality.** Vendor shall maintain a security program that is designed to protect Company’s data against unauthorized access, use, or disclosure. This includes implementing reasonable technical, administrative, and physical safeguards appropriate to the nature of the information. Vendor personnel shall only access Company data on a need-to-know basis and must adhere to confidentiality obligations. Vendor will promptly notify Company if it becomes aware of any security deficiency that materially affects the protection of Company’s data. All Company data shared with Vendor is deemed confidential, and Vendor shall not disclose it to any third party except as permitted by Company or as required by law.

**2. Incident Notification.** Vendor shall promptly inform Company of any confirmed security breach or unauthorized disclosure of Company’s sensitive data under Vendor’s custody. Such notice will be given **as soon as practicable and no later than 7 days** after discovery of the incident. The notification may be preliminary, with updated information provided as it becomes available. Vendor’s notification will describe, to the extent known, the nature of the breach, the data involved, and any steps taken to contain and investigate the incident. Vendor shall take immediate actions to prevent further access or disclosure and shall cooperate with Company’s investigation and remediation efforts. In the event any legal notifications are required to individuals or regulators, Vendor will reasonably assist Company in meeting those obligations.

**3. Security Assessments.** Upon Company’s written request (no more than annually, and in any event following any major security incident), Vendor will provide to Company a summary of its then-current information security program or responses to a reasonable security questionnaire. Vendor will also furnish copies of any relevant independent security certifications or audit reports (such as a SOC 2 report) that Vendor is willing or able to share. Company may, at its own expense and with reasonable prior notice to Vendor, conduct a remote assessment (or on-site visit if agreed by the parties) to evaluate Vendor’s compliance with this Agreement’s data protection requirements. Vendor shall address any material findings or deficiencies identified by such assessment within a reasonable timeframe. All information disclosed by Vendor during such assessments shall be treated as Vendor’s confidential information.

**4. Subcontractors.** Vendor may use subcontractors to carry out its obligations under this Agreement. In cases where a subcontractor will have access to Company’s confidential data (including any PHI), Vendor will ensure that such subcontractor is bound by contractual obligations at least as protective of the data as those imposed on Vendor hereunder. Vendor remains fully liable for the acts and omissions of its subcontractors. Upon Company’s request, Vendor will provide information regarding any major subcontractors involved in handling Company data. Vendor shall promptly notify Company of any unauthorized use or disclosure of Company data by a subcontractor of which it becomes aware, and take reasonable measures to prevent a recurrence.

**5. HIPAA Business Associate Provisions.** **[This Section applies only if Vendor will create, receive, maintain, or transmit PHI on Company’s behalf.]** The parties acknowledge that for any such activities, Company is a Covered Entity and Vendor is a Business Associate as defined by HIPAA. Vendor agrees to comply with the applicable requirements of the HIPAA Privacy and Security Rules and will only use or disclose PHI as permitted by Company and by law. Vendor shall implement appropriate safeguards to protect Electronic PHI in compliance with 45 C.F.R. §164.306 et seq. and report to Company any unauthorized use or disclosure of PHI of which it becomes aware. Vendor shall ensure that any subcontractor assisting in the fulfillment of Vendor’s services and who will have access to PHI agrees to the same restrictions and conditions that apply to Vendor with respect to such information. The parties will enter into a separate Business Associate Agreement to further detail their HIPAA obligations. If Vendor is not handling any PHI under this Agreement, this Section 5 shall not apply.

**6. Termination for Breach.** In the event that either party materially breaches this Agreement, the non-breaching party may give written notice describing the breach. The breaching party shall have **30 days** from receipt of such notice to cure the breach to the non-breaching party’s reasonable satisfaction. If the breach is cured within the cure period, the Agreement shall continue in full force. If the breaching party fails to cure the breach within 30 days, the non-breaching party may terminate this Agreement for cause by providing written notice of termination. Notwithstanding the foregoing, Company may immediately terminate this Agreement upon a material breach by Vendor that is incapable of cure or if required to do so by regulatory authorities. Upon termination or expiration of this Agreement, Vendor will return or destroy (at Company’s direction) all Company confidential data in Vendor’s possession and certify in writing that it has done so, except where retention is required by applicable law.

**7. Liability Limitations.** Except for amounts due pursuant to Section 8 (Indemnification) and for damages arising from Vendor’s intentional misconduct, each party’s total liability to the other for any claims arising out of or relating to this Agreement shall not exceed in the aggregate the fees paid or payable by Company to Vendor under this Agreement in the **twelve (12) months** prior to the event giving rise to liability. In no event shall either party be liable to the other for any indirect, consequential, special, or punitive damages arising from this Agreement, even if advised of the possibility of such damages. The limitations in this section shall not apply to any liability which cannot be limited by law.

**8. Indemnification.** Vendor shall indemnify and hold harmless Company and its officers, directors, and employees from any third-party claim or legal action to the extent caused by Vendor’s negligence or willful misconduct resulting in an unauthorized disclosure of Company’s confidential data or a breach of PHI. This indemnification obligation includes reimbursement for reasonable attorneys’ fees and settlement costs incurred by Company in connection with such claim. Company shall give Vendor prompt written notice of any claim for which indemnity is sought and shall cooperate in the defense. Vendor shall have the right to control the defense and settlement of any such claim, provided that no settlement imposing any admission or non-monetary obligation on Company shall be made without Company’s prior written consent. **Limit:** Vendor’s obligations to indemnify are subject to the limitation of liability in Section 7 above. If Company’s actions or omissions contributed to the cause of the claim, any indemnification obligation of Vendor may be proportionately reduced.

**9. Signatures.**

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by their duly authorized representatives as of the date first written above.

[Company Name] [Vendor Name]

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_