BUSINESS ASSOCIATE AGREEMENT

Under the Health Insurance Portability and Accountability Act (HIPAA), as amended by the HITECH Act and the HIPAA Omnibus Rule

SAMPLE · NOT FOR EXECUTION

This Business Associate Agreement ("Agreement") is entered into by and between **[COVERED ENTITY LEGAL NAME]** ("Covered Entity") and **SecureLynx, LLC**, a California limited liability company ("Business Associate"), effective as of **[EFFECTIVE DATE]** (the "Effective Date"). Covered Entity and Business Associate may be referred to individually as a "Party" and collectively as the "Parties."

Recitals

A. Business Associate provides **[DESCRIBE SERVICES, e.g., managed IT, security, backup, and support services]** to Covered Entity under a separate services agreement (the "Underlying Agreement"), and in connection with those services may create, receive, maintain, or transmit Protected Health Information on behalf of Covered Entity.

B. The Parties intend to comply with the Privacy, Security, and Breach Notification Rules at 45 C.F.R. Parts 160 and 164 (the "HIPAA Rules"), and this Agreement sets out the terms governing Business Associate's handling of Protected Health Information.

C. This Agreement supplements and is incorporated into the Underlying Agreement. In the event of a conflict regarding Protected Health Information, the terms of this Agreement control.

NOW, THEREFORE, in consideration of the mutual promises below, the Parties agree as follows:

1. Definitions

Capitalized terms used but not defined in this Agreement have the meanings given to them in the HIPAA Rules. For convenience:

(a) "Protected Health Information" ("PHI") and "Electronic Protected Health Information" ("ePHI") have the meanings in 45 C.F.R. § 160.103, limited to information Business Associate creates, receives, maintains, or transmits for or on behalf of Covered Entity.

(b) "Breach," "Security Incident," "Required by Law," "Unsecured PHI," "Subcontractor," "Data Aggregation," and "Designated Record Set" have the meanings given in the HIPAA Rules.

(c) "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164, as amended.

2. Obligations of Business Associate

Business Associate agrees to:

(d) Not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.

(e) Use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 (the Security Rule) with respect to ePHI, to prevent use or disclosure of PHI other than as provided by this Agreement, including administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI.

(f) Report to Covered Entity any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, any Security Incident, and any Breach of Unsecured PHI, without unreasonable delay and in no event later than seventy-two (72) hours after discovery. Such report shall include, to the extent known, the information required under 45 C.F.R. § 164.410, including the individuals affected and the nature of the incident. The Parties acknowledge this Section as notice of the ongoing occurrence of unsuccessful Security Incidents (such as routine, unsuccessful access attempts and pings) for which no additional notice is required.

(g) In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), ensure that any Subcontractor that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees in writing to restrictions and conditions at least as protective as those that apply to Business Associate under this Agreement.

(h) Make available PHI in a Designated Record Set to Covered Entity, or as directed by Covered Entity to an individual, as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524 (access).

(i) Make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by Covered Entity, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526 (amendment).

(j) Maintain and make available the information required to provide an accounting of disclosures to Covered Entity or an individual as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.528 (accounting of disclosures).

(k) To the extent Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 C.F.R. Part 164, comply with the requirements of that Subpart that apply to Covered Entity in the performance of those obligations.

(l) Make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance with the HIPAA Rules.

SAMPLE - NOT FOR EXECUTION

3. Permitted Uses and Disclosures by Business Associate

(m) Business Associate may use or disclose PHI only as necessary to perform the services set out in the Underlying Agreement, as required by this Agreement, or as Required by Law.

(n) Business Associate may use PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities.

(o) Business Associate may disclose PHI for its proper management and administration or to carry out its legal responsibilities only if the disclosure is Required by Law, or if Business Associate obtains reasonable assurances from the recipient that the PHI will remain confidential and be used or further disclosed only as Required by Law or for the purpose disclosed, and that the recipient will notify Business Associate of any breach of confidentiality.

(p) Business Associate may provide Data Aggregation services relating to the health care operations of Covered Entity where permitted by 45 C.F.R. § 164.504(e)(2)(i)(B), and may de-identify PHI in accordance with 45 C.F.R. § 164.514(a)-(c), only if expressly permitted in writing by Covered Entity.

(q) Business Associate shall not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except as set out in this Section.

(r) Business Associate shall limit its use, disclosure, and request of PHI to the minimum necessary to accomplish the intended purpose, in accordance with 45 C.F.R. § 164.502(b) and any minimum-necessary policies the Covered Entity communicates to Business Associate.

4. Obligations of Covered Entity

(s) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(t) Covered Entity shall notify Business Associate of any changes in, or revocation of, an individual's permission to use or disclose PHI, to the extent that such change may affect Business Associate's use or disclosure of PHI.

(u) Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(v) Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permitted under Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except as permitted under Section 3.

5. Term and Termination

(w) Term. This Agreement is effective as of the Effective Date and continues until the later of the termination of the Underlying Agreement or the date Business Associate returns or destroys all PHI as provided below.

SAMPLE - NOT FOR EXECUTION

(x) Termination for Cause. Covered Entity may terminate this Agreement and the Underlying Agreement if it determines that Business Associate has materially breached this Agreement and Business Associate has failed to cure the breach within thirty (30) calendar days of written notice, or if cure is not possible, Covered Entity may terminate immediately.

(y) Effect of Termination. On termination, Business Associate will return or destroy all PHI it maintains for Covered Entity within fifteen (15) days, and retain no copies, except where such return or destruction is infeasible. The Parties acknowledge that PHI contained in immutable, Object Lock protected backup copies cannot be returned or destroyed before the applicable retention period expires (up to six (6) months from the date each copy was created). For such PHI, Business Associate will: (i) retain no copies other than those so protected; (ii) not access or use the retained PHI except as Required by Law or to maintain its security; (iii) extend the protections of this Agreement to that PHI for as long as it is retained; and (iv) permanently destroy the PHI on expiry of the immutability retention period. This reflects the infeasibility exception under HIPAA's business associate contract requirements at 45 C.F.R. § 164.504(e).

6. Breach Notification and Cooperation

(z) Business Associate shall cooperate with Covered Entity in meeting Covered Entity's obligations under the Breach Notification Rule (45 C.F.R. §§ 164.400-414), including by providing the information needed for Covered Entity to notify affected individuals, the Secretary, and, where applicable, the media within the timeframes required by law.

(aa) Unless otherwise agreed in writing, Covered Entity is responsible for providing legally required notifications to affected individuals. The Parties shall reasonably cooperate to mitigate, to the extent practicable, any harmful effect known to them of a use or disclosure of PHI in violation of this Agreement.

7. Miscellaneous

(bb) Regulatory References. A reference in this Agreement to a section of the HIPAA Rules means the section as in effect or as amended.

(cc) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(dd) Interpretation. Any ambiguity in this Agreement shall be resolved to permit the Parties to comply with the HIPAA Rules.

(ee) No Third-Party Beneficiaries. Nothing in this Agreement confers any rights upon any person other than the Parties and their respective successors and permitted assigns.

(ff) Survival. The obligations of Business Associate under Section 5 (Effect of Termination) survive the termination of this Agreement.

SAMPLE · NOT FOR EXECUTION

(gg) Governing Law. This Agreement is governed by the laws of the State of California and applicable federal law, without regard to conflict-of-laws principles.

(hh) Counterparts. This Agreement may be executed in counterparts, including by electronic signature, each of which is deemed an original and all of which together constitute one agreement.

Signatures

IN WITNESS WHEREOF, the Parties have executed this Business Associate Agreement as of the Effective Date.

COVERED ENTITY

_____

Signature

[COVERED ENTITY LEGAL NAME]
By (print name): **[NAME]**
Title: **[TITLE]**
Date: **[DATE]**

BUSINESS ASSOCIATE

_____

Signature

SecureLynx, LLC
By (print name):
Title: Founder
Date: **[DATE]**

SAMPLE · NOT FOR EXECUTION