



NOTE: This sample agreement is drafted to comply with the HIPAA rules as amended January 2013, and contains terms that are *slightly more favorable to business associates*. Covered entities should consider adopting a different version that is more favorable to covered entities. The agreement should be reviewed and modified to fit the user's circumstances and satisfy any additional state or federal laws that may apply to the user. Optional but recommended language appears in italics.

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered between _____ ("Covered Entity") and _____ ("Business Associate").

Background

Pursuant to the parties' separate services agreement ("Services Agreement"), Business Associate has agreed to perform certain services for or on behalf of Covered Entity that may involve the creation, maintenance, use, transmission or disclosure of protected health information within the meaning of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and its implementing regulations, 45 CFR Parts 160 and 164 ("HIPAA Rules"). This Agreement supplements the Services Agreement and is intended to and shall be interpreted to satisfy the requirements for business associate agreements as set forth in the HIPAA Rules as they shall be amended.

Definitions

1. **General Definitions.** The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: *Breach, Data Aggregation, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.*

2. **Specific Definitions.**

a. **Business Associate** shall generally have the same meaning as the term "business associate" at 45 CFR § 160.103, and in reference to the party to this Agreement, shall mean Business Associate.

b. **Covered Entity** shall generally have the same meaning as the term "covered entity" at 45 CFR § 160.103, and in reference to the party to this Agreement, shall mean Covered Entity.

c. **Protected Health Information** shall generally have the same meaning as the term "protected health information" at 45 CFR § 160.103, and shall include any individually identifiable information that is created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity that relates to an individual's past, present, or future physical or mental health, health care, or payment for health care, whether such information is in oral, hard copy, electronic, or any other form or medium.

Agreement

1. **Business Associate Responsibilities.** Business Associate agrees to:



a. Not use or disclose protected health information except as permitted by Section 2, below, or as otherwise required by law.

b. Use appropriate safeguards to prevent the use or disclosure of protected health information other than as permitted by this Agreement. To the extent applicable to business associates, Business Associate shall comply with the requirements in 45 CFR Part 164, Subpart C, including the use of administrative, physical and technical safeguards to protect electronic protected health information.

c. Report to Covered Entity any use or disclosure of protected health information not permitted by this Agreement of which it becomes aware, including breaches of unsecured protected health information as required by 45 CFR § 164.410, and any security incident as required by 45 CFR § 164.314(a)(2). The parties acknowledge that Business Associate is periodically subject to attempted but unsuccessful attempts to access its information system (e.g., typical "pings" or port scans), but that such unsuccessful attempts are trivial, routine, and do not constitute a material threat to the security of protected health information. The parties agree that further notice of such trivial but unsuccessful attempts shall not be required unless expressly required by Covered Entity.

d. Ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information as required by 45 CFR §§ 164.502(e)(1) and (2) and 164.308(b)(2). Business Associate may fulfill this requirement by having the subcontractors execute an agreement that incorporates the terms of this Agreement.

e. Within fifteen (15) days after Covered Entity's request, make available to Covered Entity any protected health information in Business Associate's control as necessary to enable Covered Entity to satisfy its obligations to provide an individual with access to certain protected health information under 45 CFR § 164.524.

f. Within thirty (30) days after Covered Entity's request, make available to Covered Entity any protected health information for amendment and incorporate any amendments to protected health information as necessary to enable Covered Entity to satisfy its obligations under 45 CFR § 164.526.

g. Within thirty (30) days after Covered Entity's request, make available to Covered Entity the information required to provide an accounting of disclosures as necessary to enable Covered Entity to satisfy its obligations under 45 CFR § 164.528.

h. To the extent Business Associate is to carry out Covered Entity's obligations under 45 CFR Part 164, Subpart E, comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligations.

i. Make Business Associate's internal practices, books, and records relating to the use and disclosure protected health information received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Rules.

2. Uses and Disclosures by Business Associate.

2.1 Permissible Uses and Disclosures. Business Associate may use or disclose protected health information only as follows:

a. As necessary to perform the services set forth in the Service Agreement.



b. To de-identify protected health information in accordance with 45 CFR § 164.514(a)-(c). Any information that has been de-identified as provided in this subsection shall not be subject to this Agreement.

c. As required by law.

d. For the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that: (i) any disclosures for these purposes are required by law, or (ii)(a) Business Associate obtains reasonable assurances from the entity to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the entity, and (b) the entity notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

e. To provide data aggregation services relating to the health care operations of Covered Entity as defined in 45 CFR § 164.501.

2.2 Impermissible Uses or Disclosures. Business Associate may not use or disclose protected health information in a manner that would violate 45 CFR Part 164, Subpart E, if done by Covered Entity except for the specific uses and disclosures set forth in Sections 2.1(d)-(e), above.

2.3 Minimum Necessary. Business Associate agrees to make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures as disclosed by Covered Entity to Business Associate in advance.

3. Covered Entity Responsibilities. Covered Entity shall notify Business Associate of limitations on the use or disclosure of protected health information as follows:

a. Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.

b. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect Business Associate's use or disclosure of protected health information.

c. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that Covered Entity has agreed to or is required to abide by under 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

4. Requests by Covered Entity. Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permitted under 45 CFR Part 164, Subpart E, if done by Covered Entity, except that Business Associate may use or disclose protected health information for Business Associate's data aggregation, management, administration, and legal responsibilities as set forth in Section 2.1(d)-(e).

5. Term and Termination. Unless otherwise agreed in writing by the parties, this Agreement shall be effective as of the date executed by the parties and shall continue until terminated as provided below.

5.1 Termination. This Agreement may be terminated as follows:



a. Either party may terminate this Agreement upon thirty (30) days prior written notice to the other party due to a material breach of this Agreement by the other party. The breaching party shall have the opportunity to cure the breach during the 30-day notice period. If the breaching party fails to cure the breach within the 30-day notice period, the non-breaching party may declare the Agreement terminated by providing written notice at the end of the 30-day period.

b. Either party may terminate this Agreement if either party determines that the other party has violated any law or regulation and/or that continued performance under this Agreement may subject the party to adverse action by any governmental agency.

5.2 Obligations of Business Associate Upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

a. Retain only that protected health information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities as described in Section 2.1(d).

b. If feasible, return or destroy all other protected health information in Business Associate's control.

c. For any protected health information that is retained, continue to extend the protections of this Agreement to such information and limit further uses and disclosures to those purposes permitted by this Agreement.

5.3 Survival. Business Associate's obligations under this Section shall survive the termination of this Agreement.

6. Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

7. Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary to comply with the requirements of the HIPAA Rules and any other applicable law.

8. Governing Law. This Agreement shall be construed to comply with the requirements of the HIPAA Rules, and any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules. All other aspects of this Agreement shall be governed under the laws of the State in which Business Associate maintains its principal place of business.

9. Assignment/Subcontracting. This Agreement shall inure to the benefit of and be binding upon the parties and their respective legal representatives, successors and assigns. Business Associate may assign or subcontract rights or obligations under this Agreement to subcontractors or third parties without the express written consent of Covered Entity. Covered Entity may assign its rights and obligations under this Agreement to any successor or affiliated entity.

10. Cooperation. The parties agree to cooperate with each other's efforts to comply with the requirements of the HIPAA Rules and other applicable laws; to assist each other in responding to and mitigating the effects of any breach of protected health information in violation of HIPAA Rules or this Agreement; and to assist the other party in responding to any investigation, complaint, or action by any government agency or third party relating to the performance of this Agreement.



11. **Relation to Services Agreement.** This Agreement supplements the Services Agreement. The terms and conditions of the Services Agreement shall continue to apply to the extent not inconsistent with this Agreement. If there is a conflict between this Agreement and the Services Agreement, this Agreement shall control.

12. **No Third Party Beneficiaries.** Nothing in this Agreement is intended to nor shall it confer any rights on any other persons except Covered Entity and Business Associate and their respective successors and assigns.

13. **Entire Agreement.** This Agreement contains the entire agreement between the parties as it relates to the use or disclosure of protected health information, and supersedes all prior discussions, negotiations and services relating to the same to the extent such other prior communications are inconsistent with this Agreement.

[Optional: 14. Indemnification. If a party to this Agreement breaches any provision of this Agreement or violates any requirement of the HIPAA Rules applicable to the that party, that party shall indemnify, hold harmless and defend the other party from and against any and all claims, losses, liabilities, costs and other expenses incurred by the other party as a result of such breach or violation.]

[Optional: 15. Limitation on Liability. In no event shall Business Associate or any of its directors, officers, agents, parents, affiliates or subsidiaries (collectively "Business Associate") be liable to Covered Entity or any third party for any special, consequential, incidental, or indirect loss or damages arising out Business Associate's acts or omissions relating to this Agreement or the HIPAA Rules whether or not Business Associate has been advised of the possibility of such loss or damages. In all cases, Business Associate's aggregate liability under any legal theory, including contract, tort, or other bases, shall not exceed the fees paid by Covered Entity to Business Associate pursuant to the Services Agreement during the six (6) month period prior to the first occurrence upon which liability is based.]

Comment [KS1]: Coordinate with services agreement, and consider appropriate limitations on indemnification requirements, e.g., reduction by the CE's fault, limit to available insurance, etc

Comment [KS2]: Coordinate with services agreement, and consider appropriate limitations on indemnification requirements, e.g., reduction by the CE's fault, limit to available insurance, etc.

COVERED ENTITY

By: _____
Print Name: _____
Print Title: _____
Date: _____

BUSINESS ASSOCIATE

By: _____
Print Name: _____
Print Title: _____
Date: _____