# SAMPLE

# BUSINESS ASSOCIATE AGREEMENT

***This is a draft business associate agreement based on the template provided by HHS. It is not intended to be used as is and you should only use the agreement after you have reviewed it with your legal counsel. O.C.A Benefit Services, LLC does not, nor is it authorized to, provide legal advice, and the fact that we have provided a sample document should not be construed as such.***

## Instructions

1. Fill in the name of your company, the client company's name and the name of the applicable group health plan sponsored by the client for which you will be receiving protected health information where indicated by the red, bracketed text. You will need this information in:

    - The lead-in paragraph;
    - Section 1.3;
    - Section 1.4; and
    - Above the signature lines.

2. Fill in the list of purposes for which you may use protected health information shown in red, bracketed text under Section 3.1(b). If this information is specified in a services agreement between your company and the client, Section 3.1(a) will govern and a list of purposes is not required in Section 3.1(b).

3. The agreement is effective as of the later date signed, so make sure both parties sign and date the agreement.

# Business Associate Contract

Effective as of the date set forth below (the "Effective Date"), **[Insert Broker company name]** and **[Insert client name]**, as plan administrator of the **[Insert name of client's group health plan]** (the "Plan") hereby enter into this business associate contract ("BA Contract") as set forth herein.

## I. Definitions

Terms used, but not otherwise defined, in this Agreement shall have the same meaning given those terms under HIPAA.

1.1 Agreement. "Agreement" means the administrative services agreement entered into between Business Associate and Covered Entity pursuant to which Business Associate provides services to the Plan.

1.2 Breach. "Breach" shall have the same meaning as the term "breach" in 45 CFR § 164.402.

1.3 Business Associate. "Business Associate" means **[Insert Name of Broker Company]**.

1.4 Covered Entity. "Covered Entity" means **[Insert Name of health plan sponsored by Client]**.

1.5 Electronic Protected Health Information. "Electronic Protected Health Information" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103.

1.6 Electronic Transaction Rule. "Electronic Transaction Rule" means the final regulations issued by HHS concerning standard transactions and code sets under 45 CFR Parts 160 and 162.

1.7 HHS. "HHS" means the United States Department of Health and Human Services.

1.8 HIPAA. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as amended, and the accompanying regulations.

1.9 Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

1.10 Privacy Rule. "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

1.11 Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

1.12 Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

1.13 Secretary. "Secretary" means the Secretary of the Department of Health and Human Services or his designee.

1.14 Security Rule. "Security Rule" means the Security Standards and Implementation Specifications at 45 CFR §§ 164.306, 164.308, 164.310, 164.312, and 164.316.

1.15 Security Incident. "Security Incident" shall have the same meaning as the term "security incident" in 45 CFR § 164.304.

1.16 Unsecured Protected Health Information. "Unsecured Protected Health Information" shall have the same meaning as the term "unsecured protected health information" in 45 CFR § 164.402.

## II. Obligations and Activities of Business Associate

2.1 Business Associate agrees not to use or disclose Protected Health Information other than as permitted or required by this BA Contract or as Required by Law.

2.2 Business Associate agrees to develop, implement, maintain and use appropriate administrative, technical and physical safeguards to prevent use or disclosure of the Protected Health Information, other than as provided for by this BA Contract.

2.3 Business Associate will develop, implement, maintain and use administrative, technical and physical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information that Business Associate creates, receives, maintains or transmits on Covered Entity's behalf as required by the Security Rule.

2.4 Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this BA Contract.

2.5 Business Associate agrees to report to Covered Entity any use or disclosure of Protected Health Information, including Electronic Protected Health Information, not provided for by this BA Contract of which it becomes aware and/or any Security Incident of which it becomes aware.

2.6 Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information and/or Electronic Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this BA Contract to Business Associate with respect to such information. Moreover, Business Associate shall ensure that any such subcontractor or agent agrees to implement reasonable and appropriate safeguards to protect Covered Entity's Protected Health Information.

2.7 As of the effective date specified by HHS in final regulations to be issued on this topic, Business Associate shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an individual unless the Covered Entity or Business Associate obtains from the individual, in accordance with 45 CFR § 164.508, a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by the entity receiving Protected Health Information of that individual, except as otherwise allowed under HIPAA.

2.8 To the extent it maintains a Designated Record Set, Business Associate agrees to provide access, at the request of Covered Entity, as soon as administratively practical and in no event later than 30 days following the Covered Entity's request, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524.

2.9 To the extent it maintains a Designated Record Set, Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, as soon as administratively practicable.

2.10 Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected

Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

2.11 Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

2.12 Business Associate agrees to provide to Covered Entity or an Individual, within 30 days following Covered Entity's request, information collected in accordance with the Agreement and/or this BA Contract, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

2.13 If Business Associate conducts in whole or in part electronic transactions on behalf of Covered Entity for which HHS has established standards, Business Associate will comply, and will require any subcontractor to comply, with each applicable requirement of the Electronic Transaction Rule. Business Associate shall also comply with the National Provider Identifier requirements, if and to the extent applicable.

2.14 Business Associate acknowledges that it is subject to civil and criminal enforcement for failure to comply with the Privacy Rule and Security Rule.

## III. Permitted Uses and Disclosures by Business Associate

3.1 General Use and Disclosure Provisions.

(a) Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities or services for, or on behalf of, Covered Entity as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

(b) In the event Business Associate and Covered Entity have not entered into a services agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:

**[List Purposes]**.

(c) Business Associate will, in its performance of the functions, activities, services and operations specified above, make reasonable efforts to use, to disclose and to request only the minimum amount of Covered Entity's Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that Business Associate will not be obligated to comply with this minimum necessary limitation if neither Business Associate nor Covered Entity is required to limit its use, disclosure or request to the minimum necessary. Business Associate and Covered Entity acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with the Health Information Technology for Economic and Clinical Health Act ("HITECH") and government guidance on the definition.

3.2 Specific Use and Disclosure Provisions.

(a) Except as otherwise limited in this BA Contract, Business Associate may use Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

(b) Except as otherwise limited in this BA Contract, Business Associate may disclose Protected Health Information for the proper management and administration of Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Except as otherwise limited in this BA Contract, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

(d) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1).

## IV. Obligations of Covered Entity

4.1 Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions.

(a) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 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, permission by an Individual to use or disclose 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 to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information. Covered Entity shall not agree to any restrictions without the written consent of Business Associate except with respect to a restriction where (1) the disclosure is to a health plan for purposes of carrying out payment or health care operations, and (2) the Protected Health Information pertains solely to a health care item or service for which the health care provider involved has been paid in full out of pocket.

4.2 Permissible 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 permissible under the Privacy Rule if done by Covered Entity, except that Business Associate may use or disclose Protected Health Information for purposes of data aggregation.

## V. Breaches and Security Incidents

5.1 Privacy or Security Breach. Business Associate will report to Covered Entity any use or disclosure of Covered Entity's Protected Health Information not permitted by this BA Contract along with any Breach of Covered Entity's Unsecured Protected Health Information. Business Associate will treat the Breach as being discovered in accordance with 45 CFR § 164.410. Business Associate will make the report to Covered entity's Privacy Official or other corporate contract within 60 calendar days after Business Associate learns of such non-permitted use or disclosure. If a delay is requested by a law-enforcement official in accordance with 45 CFR § 164.412, Business Associate may delay notifying Covered Entity for the applicable time period. Business Associate's report will at least:

(a) Identify the nature of the breach or other non-permitted use or disclosure, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of any Breach;

(b) Identify Covered Entity's Protected Health Information that was subject to the non-permitted use or disclosure or Breach (such as whether full name, social security number, date of birth, home address, account number or other information were involved) on an individual basis;

(c) Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure;

(d) Identify what corrective or investigational action Business Associate took or will take to prevent further non-permitted uses or disclosures, to mitigate harmful effects and to protect against any further Breaches;

(e) Identify what steps the individuals who were subject to a Breach should take to protect themselves;

(f) Provide such other information, including a written report, as Covered Entity may reasonably request.

5.2 Security Incidents. Business Associate will report to Covered Entity any successful (A) unauthorized access, use, disclosure, modification, or destruction of Covered Entity's Electronic Protected Health Information or (B) interference with Business Associate's system operations in Business Associate's information systems, of which Business Associate becomes aware. Business Associate will make this report monthly, except that if any such Security Incident resulted in a disclosure not permitted by this BA Contract or Breach of Covered Entity's Unsecured Protected Health Information, Business Associate will make the report in accordance with the provisions set forth in the paragraph above.

## VI. Term and Termination

6.1 Term. The Term of this BA Contract shall be effective as of Effective Date, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

6.2 Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

(a) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Agreement and/or this BA Contract if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(b) Immediately terminate the Agreement and/or this BA Contract if Business Associate has breached a material term of this BA Contract and cure is not possible; or

(c) If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

6.3 Effect of Termination.

(a) Except as provided in paragraph (b) of this section, upon termination of this BA Contract, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(b) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon notifying Covered Entity that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this BA Contract to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

## VII. Miscellaneous

7.1 Regulatory References. A reference in this BA Contract to a section in the Privacy Rule or the Security Rule means the section as in effect or as amended.

7.2 Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity and/or Business Associate to comply with the requirements of the Privacy Rule, and, the Security Rule and any other provision of HIPAA.

7.3 Survival. The respective rights and obligations of Business Associate under Section 6.3 of this BA Contract shall survive the termination of this BA Contract.

7.4 Interpretation. Any ambiguity in this BA Contract shall be resolved to permit Covered Entity and/or Business Associate to comply with HIPAA.

**[SIGNATURES FOLLOW ON NEXT PAGE]**

IN WITNESS WHEREOF, the parties have duly executed this BA Contract effective as of the later date signed below.

**[BROKER COMPANY NAME]**

By: _____

Name: _____

Title: _____

Date Signed: _____

**[CLIENT NAME]**

By: _____

Name: _____

Title: _____

Date Signed: _____