

This Business Associate Agreement (the "Agreement") is entered into by and between \_\_\_\_\_ (the "Plan") **{or Plan Sponsor if Underlying Agreement is with Plan Sponsor, not Plan}** and eflexgroup, Inc./eCOBRA (together referred to as the "Business Associate") effective February 17, 2010 or date document is signed.

WHEREAS, the Plan is a group health plan as defined in Title 45, Parts 160 and 164 of the Code of Federal Regulations (the "Privacy Regulations") and Title 45, Parts 160, 162 and 164 of the Code of Federal Regulations (the "Security Regulations") (together, the "Privacy and Security Regulations") adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA");

WHEREAS, Business Associate and the Plan **{Sponsor}** entered into an agreement ("Underlying Agreement") whereby Business Associate will perform services on behalf of the Plan; and

WHEREAS, the Parties wish to set forth their understandings with regard to the use and disclosure of Protected Health Information ("PHI") by Business Associate in performance of its obligations in compliance with (1) the Privacy and Security Regulations; and (2) Subtitle D of the Health Information Technology for Economic and Clinical Health Act, Title XIII of Public Law 111-005 (42 U.S.C.A. Section 17921 et seq., subchapter III, Privacy) and regulations promulgated there under by the U.S. Department of Health and Human Services ("DHHS") (together referred to as "HITECH").

In consideration of the mutual promises set forth below, the parties hereby agree as follows:

1. Definitions. Capitalized terms shall have the meanings given to them in the Privacy and Security Regulations and HITECH, which are incorporated herein by reference.

2. Use and Disclosure of Protected Health Information. The Plan and Business Associate hereby agree to comply with the privacy and security requirements of HIPAA, as set forth in the Privacy and Security Regulations and HITECH. Business Associate shall use and/or disclose PHI only to the extent necessary in furtherance of Business Associate's obligations and duties under the Underlying Agreement with the Plan and as authorized or permitted by the Privacy and Security Regulations and HITECH. Business Associate shall disclose PHI to other business associates of the Plan to the extent necessary for purposes of the Plan's Payment and Health Care Operations, provided such other business associates have business associate agreements in place with the Plan as required by the Privacy Regulations (and a copy of the applicable provisions of such other business associate agreements will be provided to Business Associate upon request). Business Associate shall disclose PHI to the Plan Sponsor to the extent necessary for the Plan Sponsor's administration activities that constitute Payment or Health Care Operations, provided the Plan document has been amended as required by the Privacy Regulations (and a copy of the applicable provisions of the Plan document will be provided to Business Associate upon request). Business Associate may disclose Summary Health Information to the Plan Sponsor for the purpose of (a) obtaining bids for health or stop loss insurance for the Plan, or (b) modifying, amending or terminating the Plan.

3. Prohibition on Unauthorized Use or Disclosure of PHI. Business Associate shall not use or disclose any PHI received from or on behalf of the Plan, except as permitted or required by the Underlying Agreement, this Agreement, the Privacy and Security Regulations, HITECH and as required by law or as otherwise authorized in writing by the Plan. Business Associate shall comply with the applicable provisions of: (a) the Privacy Regulations; (b) HITECH (including 42 U.S.C.A. sections 17931 and 17934); (c) state laws, rules and regulations applicable to individually-identifiable health information not preempted by federal law; and (d) the Plan's health information privacy policies and procedures.

4. Business Associate's Operations. Business Associate may use PHI it creates for or receives from the Plan, in its capacity as a Business Associate, to the extent necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities but only if:

(a) The disclosure is required by law; or

(b) Business Associate obtains reasonable assurance, evidenced by written contract, from any person or organization to which Business Associate shall disclose such PHI that such person or organization shall:

(i) Hold such PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization or as required by law; and

(ii) Notify Business Associate (who shall in turn promptly notify the Plan) of any instance of which the person or organization becomes aware in which the confidentiality of such PHI was breached as soon as possible.

5. Data Aggregation Services. Business Associate may use PHI to provide Data Aggregation Services related to the Plan's Health Care Operations.

6. PHI Safeguards. Business Associate shall develop, implement, maintain and use appropriate administrative, technical and physical safeguards to prevent the improper use or disclosure of any PHI relating to the Plan.

7. Electronic Health Information Security and Integrity. Business Associate shall develop, implement, maintain and use appropriate administrative, technical and physical security measures consistent with and in compliance with the Security Regulations and HITECH to preserve the integrity, confidentiality and availability of all electronic PHI that it creates, receives, maintains or transmits on behalf of the Plan. Business Associate shall document and keep these security measures current in accordance with the Security Regulations and HITECH (including 42 U.S.C.A. section 17931).

8. Protection of Exchanged Information in Electronic Transactions. If Business Associate conducts any Standard Transaction for or on behalf of the Plan, Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of the Privacy and Security Regulations.

9. Subcontractors and Agents. Business Associate shall require each of its subcontractors or agents to whom Business Associate may provide PHI on behalf of the Plan to agree to written contractual provisions that impose at least the same obligations to protect such PHI as are imposed on Business Associate by this Agreement, the Privacy and Security Regulations and HITECH.

10. Access to PHI. Business Associate shall provide access, at the request of the Plan, to PHI in a Designated Record Set, to the Plan or, as directed by the Plan, to an Individual to meet the requirements under Title 45, Section 164.524 of the CFR or applicable state law and to meet the electronic transmission requirements for access to Electronic Health Records by Individuals in accordance with HITECH, including 42 U.S.C.A. section 17935(e). Business Associate shall provide access in the time and manner set forth in the Plan's health information privacy policies and procedures.

11. Amending PHI. Business Associate shall make any amendment(s) to PHI in a Designated Record Set that the Plan directs or agrees to pursuant to Title 45, Section 164.526 of the CFR at the request of the Plan or an Individual in the time and manner set forth in the Plan's health information privacy policies and procedures.

## 12. Accounting for Disclosures of PHI.

(a) Business Associate shall document all disclosures of PHI and information related to such disclosures as would be required for the Plan to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with Title 45, Section 164.528 of the CFR, including PHI in Electronic Health Records in accordance with HITECH.

(b) Business Associate agrees to provide the Plan, in the time and manner set forth in the Plan's health information privacy policies and procedures, information collected in accordance with Section 12(a) above, to permit the Plan to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with Title 45, Section 164.528 of the CFR and HITECH, including 42 U.S.C.A. section 17935(c) with respect to Electronic Health Records. To the extent a request for an accounting relates to disclosures of PHI in Electronic Health Records by Business Associate, at the Plan's election, the Plan can provide an Individual who requests such accounting with Business Associate's contact information, and Business Associate shall provide the accounting directly to the Individual upon request by the Individual.

13. Access to Books and Records. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI received from or on behalf of the Plan available to the Plan and to DHHS or its designee for the purpose of determining the Plan's compliance with the Privacy Regulations and HITECH.

14. Reporting. As described below, Business Associate shall report to the Plan in writing (a) any use or disclosure of PHI not permitted under 45 CFR section 164, Subpart E, this Agreement, or by law, (b) any Security Incident of which it becomes aware and (c) any Breach of Unsecured PHI in accordance with HITECH, including 42 U.S.C.A. section 17932. For purposes of this Agreement, the term Security Incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of electronic PHI relating to the Plan.

(a) Reporting Security Incidents or Improper Uses or Disclosures. Business Associate shall make the report to the Plan's Privacy Official (or to the Plan's Security Official in the event of a Security Incident) within 3 business days after Business Associate learns of such unauthorized use or disclosure or Security Incident. Business Associate's report shall: (i) identify the nature of the unauthorized use or disclosure or Security Incident; (ii) identify the PHI affected; (iii) identify who made the unauthorized use and/or received the unauthorized disclosure and/or participated in the Security Incident, if known; (iv) identify what Business Associate has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure or Security Incident; (v) identify what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure or Security Incident; and (vi) provide such other information, including a written report, as reasonably requested by the Plan's Privacy Official or Security Official. Any Security Incident or unauthorized use or disclosure of PHI that is a Breach of Unsecured PHI shall be reported as required under subsection (b) below.

(b) Notification of a Breach. Pursuant to HITECH, including 42 U.S.C.A. section 17932, and regulations under 45 CFR Parts 160 and 164, as amended, Business Associate shall provide written notice to the Plan's Privacy Official of any Breach of Unsecured PHI within three business days after Business Associate discovers the Breach. Business Associate shall conduct the risk assessment to determine whether a Breach occurred. Business Associate's report to the Plan shall identify or describe: (i) the affected Individual whose Unsecured PHI has been or is reasonably believed to have been accessed, acquired or disclosed; (ii) the incident, including the date of the Breach and the date of the discovery of the Breach, if known; (iii) who made the unauthorized use and/or received the unauthorized disclosure; (iv) the types of Unsecured PHI involved in the Breach; (v) any specific steps the Individual should take to protect him or herself from potential harm related to the Breach; (vi) what the Business Associate is doing to investigate the Breach, to mitigate losses and to protect against further Breaches; (vii) contact procedures for how the Individual can obtain further information from Business Associate; and (viii) such other information, including the risk assessment analysis prepared by Business Associate, as reasonably requested by the Plan's Privacy Official.

15. Sale of PHI. Business Associate shall not receive direct or indirect payment in exchange for any PHI relating to the Plan or its Individuals, including Electronic Health Records, unless Business Associate receives authorization by all affected Individuals, except as permitted under HITECH including 42 U.S.C.A. section 17935(d).

16. Marketing. Business Associate shall not receive direct or indirect payment for marketing communications which include PHI relating to the Plan or its Individuals without authorization from the affected Individuals unless such communication is permitted under the Privacy Regulations and HITECH, including 42 U.S.C.A. section 17936.

17. Restrictions on Uses, Disclosures and Requests.

(a) Business Associate will limit all uses, disclosures and requests of PHI, including electronic PHI, to the Limited Data Set to the extent possible or, if that is not sufficient, then to the minimum necessary to accomplish the intended purpose of such use, disclosure or request, as required by the Privacy Regulations and HITECH (including 42 U.S.C.A. 17935(b)).

(b) Upon the request of an Individual, Business Associate will not disclose such Individual's PHI for purposes of Payment or Health Care Operations if the Individual paid in full out of pocket for the health care item or service to which the PHI relates, in accordance with HITECH (including 42 U.S.C.A. section 17935(a)).

18. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

19. Termination for Cause. As required by the Privacy Regulations and section 42 U.S.C.A. 17934, if the Plan or Business Associate ("Non-Breaching Party") becomes aware that the other entity to this Agreement has engaged in a material breach ("Breaching Party"), then the Non-Breaching Party shall:

(a) Provide an opportunity for the Breaching Party to cure the breach or end the violation and terminate this Agreement and the Underlying Agreement if the Breaching Party does not cure the breach or end the violation within the time specified by the Non-Breaching Party.

(b) Immediately terminate this Agreement and the Underlying Agreement if cure is not possible.

(c) If neither termination of this Agreement and the Underlying Agreement nor cure is feasible, report the violation to DHHS.

20. Return or Destruction of Health Information.

(a) Except as provided in Section 20(b) below, and subject to any record retention provisions of the Underlying Agreement, upon termination, cancellation, expiration or other conclusion of this Agreement and the Underlying Agreement, Business Associate shall return to the Plan or destroy all PHI created or received by Business Associate on behalf of the Plan. This provision shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate.

(b) In the event that the Parties mutually determine that returning or destroying the PHI is infeasible, Business Associate shall retain the PHI, extend the protections of this Agreement to such PHI and maintain the confidentiality of all such PHI, for so long as Business Associate maintains such PHI. The obligations of Business Associate under this Section 20(b) shall survive termination of this Agreement and the Underlying Agreement.

21. Obligations of Plan.

(a) The Plan shall provide Business Associate a copy of the Plan's Notice of Privacy Practices if there are limitations in the Notice that would prevent disclosure or use of PHI.

(b) The Plan shall notify Business Associate of any restriction to the use or disclosure of PHI that the Plan has agreed to (and any revocation of such a restriction), to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(c) The Plan shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Regulations or HITECH if done by the Plan, except as permitted in Sections 4 and 5 above.

22. Automatic Amendment. Upon the effective date of any amendment to the Privacy and Security Regulations or HITECH and any applicable regulations there under with respect to PHI, the Agreement shall automatically be deemed to be amended to incorporate such amendment to the Privacy and Security Regulations and HITECH and applicable regulations so that Business Associate and the Plan remain in compliance with the Privacy and Security Regulations and HITECH and applicable regulations.

21. Hold Harmless. Business Associate shall indemnify and hold the Plan and its employees, directors and trustees harmless from all liabilities, penalties, taxes, costs, expenses or damages of any sort resulting from or attributable to Business Associate's breach of this Agreement.

22. Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and such counterparts shall constitute one and the same instrument.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf, effective as of February 17, 2010.

**{Plan or Plan Sponsor Name}**

eflexgroup, Inc./eCOBRA

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

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

Its: \_\_\_\_\_

Its: Director of Compliance

Signed This \_\_\_\_\_ Day of \_\_\_\_\_, 20\_\_\_\_ .