HIPAA BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement ("Agreement") is entered into by the parties subject to an agreement with each other ("Underlying Agreement") whereby Business Associate performs services for Covered Entity in connection with which Business Associate may create, receive, maintain, and/or transmit Protected Health Information (as defined below) from or on behalf of Covered Entity.

WHEREAS Covered Entity and Business Associate desire to protect the privacy and security of any such Protected Health Information in compliance with the Health Insurance Portability and Accountability Act as amended (including the Health Information Technology for Economic and Clinical Health Act ["HITECH Act"] and the HIPAA Rules (as defined below; collectively "HIPAA")).

WHEREAS on Jan. 25, 2013, the U.S. Department of Health and Human Services ("HHS") issued a Final Rule (the "Omnibus Rule") containing modifications to the HIPAA Privacy Rule, the HIPAA Security Rule, and the Breach Notification Rule under HIPAA and the HITECH Act; and

WHEREAS HHS will continue to issue guidance, standards, and regulations in its ongoing role as regulatory agency for HIPAA and Health Information Technology;

NOW, THEREFORE, in consideration of the foregoing recitals, the mutual promises and covenants set forth herein, and other good and valuable consideration, Covered Entity and Business Associate agree as follows.

DEFINITIONS

The following terms shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Records Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (also referred to as "PHI"), Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

"Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR §160.103, and, with regard to this Agreement, shall mean the party who may create, receive, maintain, and/or transmit Protected Health Information from or on behalf of Covered Entity.

"Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR §160.103, and, with regard to this Agreement, shall mean the party who may have Protected Health Information created, received, maintained, and/or transmitted by Business Associate on Covered Entity's behalf.

"HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR §Parts 160, 162, and 164.

I. BUSINESS ASSOCIATE'S RESPONSIBILITIES

A. ***Permitted Access, Use, and Disclosure Compliance.*** Business Associate agrees to access, use, and disclose PHI only for the purpose of performing its obligations in the Underlying Agreement and in compliance with the Underlying Agreement, this Agreement, the provisions of HIPAA (including, without limitation, applicable portions of the Privacy, Security, Breach Notification, and Enforcement Rules), and as Required by Law. If the Underlying Agreement requires the Business Associate to perform Data Aggregation, management, or administrative activities, the Business Associate may access, use, or disclose PHI for those specific purposes.

B. ***Safeguards.*** Business Associate agrees to use appropriate administrative, technical, and physical safeguards and to comply with subpart C of 45 CFR Part 164 with respect to electronic PHI, to prevent access, use, or disclosure of PHI other than as provided for by this Agreement.

C. ***Mitigation.*** Business Associate agrees to mitigate, to the extent practicable, the harmful effects of (i) any access, use, or disclosure of PHI by Business Associate in violation of the requirements of this Agreement; and (ii) any Security Incidents.

D. ***Reports of Improper Access, Use, or Disclosure.*** Business Associate agrees to report to Covered Entity any access, use, or disclosure of PHI not permitted by this Agreement if the access, use, or disclosure results or may have resulted in any Breach. All such reports shall be provided in accordance with any notice provision in the Underlying Agreement with a copy to HealthPlanCPO@upmc.edu where applicable.

E. ***Security Incident.*** The Business Associate further agrees to report to the Covered Entity any Security Incident of which it becomes aware if the security incident results or may have resulted in any Breach. All such reports shall be provided in accordance with any notice provision in the Underlying Agreement with a copy to HealthPlanCPO@upmc.edu where applicable.

F. ***Notification of Breach.*** Business Associate agrees to report to Covered Entity any Breach of unsecured PHI (as defined in 45 CFR §164.402) as quickly as possible after the discovery of the Breach. In no circumstance shall this report be beyond two (2) business days from the discovery of the Breach. As soon as the names of each Individual affected are known, Business Associate shall notify the Covered Entity (in accordance with any notice provision in the Underlying Agreement with a copy to HealthPlanCPO@upmc.edu where applicable) and include all required elements for the notification that the Covered Entity must send to the Individual. To the extent the required elements are not available at the time the Breach is reported to the Covered Entity, Business Associate shall report such information to the Covered Entity as soon as it becomes available. The required elements are included in 45 CFR §164.404(c). The parties may agree, in writing, to have Business Associate complete the notification requirements.

G. ***Subcontractors and Agents.*** To the extent Business Associate uses any subcontractor or agent to provide services under the Underlying Agreement, and such subcontractor or agent creates, maintains, receives, transmits, or accesses PHI, Business Associate will require each subcontractor or agent to enter into a contract with terms that are substantially similar to the terms set forth herein.

H. ***Access to Information in a Designated Record Set, Electronic Health Record.*** If Business Associate maintains PHI in a Designated Record Set, Business Associate agrees to provide access—at the request of Covered Entity and in a reasonable time and manner designated by Covered Entity—to the PHI in the Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements of 45 CFR §164.524. If Business Associate maintains PHI in an Electronic Health Record, Business Associate agrees to provide such information in a reasonable time and manner, in an electronic format, to enable Covered Entity to fulfill its obligations under the HITECH Act.

I. ***Amending Information in a Designated Record Set.*** If Business Associate maintains PHI in a Designated Record Set, Business Associate agrees to make any amendments to PHI in a Designated Record Set at the request of Covered Entity within a time frame mutually agreed upon by the parties, and to take any other measure necessary to satisfy Covered Entity's obligations under 45 CFR §164.526.

J. ***Access to Business Associate's Books.*** Business Associate agrees to make internal practices, books, and records—including policies and procedures relating to the access, use, and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity—available to the Covered Entity (including Covered Entity's authorized agents and/or subcontractors) and/or the Secretary in a reasonable time and manner designated by Covered Entity and/or the Secretary for the purpose of the Secretary determining Covered Entity's compliance with HIPAA.

K. ***Record of PHI Disclosures.*** Business Associate agrees to document required disclosures of PHI by recording (i) the date of disclosure; (ii) the name and address of the person or entity to whom the disclosure was made; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the basis for the disclosure and a copy of the request for disclosure and authorization for disclosure, if one was required, as required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528 and the HITECH Act.

L. ***Minimum Necessary Access, Use and Disclosure.*** When accessing, using, or disclosing PHI, or when requesting PHI from the Covered Entity and/or a business associate, Business Associate agrees to make reasonable efforts to limit PHI to the minimum amount necessary to accomplish the intended purpose of the request, use, or disclosure.

M. ***Data Aggregation Services.*** Business Associate agrees to provide data aggregation services if requested by Covered Entity.

N. ***Remedies in Event of Contractual Breach.*** Business Associate expressly acknowledges and agrees that the breach of any contractual provision of this Agreement may cause irreparable harm to Covered Entity and that Covered Entity may not have an adequate remedy at law. Therefore, Business Associate agrees that, upon such contractual breach, Covered Entity is

entitled to seek injunctive relief to prevent Business Associate from commencing or continuing such contractual breach without posting bond or other security and without having to prove the inadequacy of any other available remedies. Business Associate further agrees to indemnify Covered Entity for any and all actual costs and expenses incurred as a result of Business Associate's contractual breach, including reasonable attorney's fees. These remedies and indemnifications are in addition to any remedies and indemnifications to which Covered Entity may be entitled under the Underlying Agreement.

O. ***Examination.*** Covered Entity or its authorized agents or contractors may, at Covered Entity's expense and upon advance notice to Business Associate and during Business Associate's normal business hours, examine Business Associate's facilities, systems, procedures, and records as may be necessary to certify that they are compliant with HIPAA.

II. Permitted Access, Use, and Disclosures by Business Associate

A. Except as otherwise limited in this Agreement, Business Associate may access, use, or disclose PHI for the purpose of fulfilling any responsibilities it may have with any employer groups that are included under a previously executed agreement or that the Business Associate has with the Covered Entity, provided that such access, use, or disclosure would not violate the Privacy Rule if done by the Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

B. Except as otherwise limited in this Agreement, Business Associate may access or use PHI for the proper management and administration of the Business Associate or for carrying out the legal responsibilities of the Business Associate as delineated in this Agreement and the Underlying Agreement with the Covered Entity.

C. Except as otherwise limited in this Agreement, Business Associate may disclose PHI possessed by Business Associate in its capacity as a Business Associate of Covered Entity for the proper management and administration of Business Associate or for carrying out the legal responsibilities of Business Associate if the disclosure is required by law or if Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to such person, and such person agrees to notify Business Associate of any instances of which such person is aware that the confidentiality of the information has been breached.

D. Except as otherwise limited in this Agreement, Business Associate may access and use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 CFR §164.504(e)(2)(i)(B).

E. Business Associate may disclose PHI pursuant to 45 CFR §164.512.

F. Business Associate shall acquire no title or rights to the Covered Entity PHI, including any de-identified information, as a result of this Agreement.

G. Business Associate shall not directly or indirectly receive remuneration in exchange for any of the Covered Entity PHI.

H. Business Associate shall not directly or indirectly perform marketing to the Covered Entity's members using the Covered Entity PHI that was either provided by the Covered Entity or created or otherwise acquired by Business Associate on behalf of the Covered Entity.

I. Business Associate shall agree to Security Standards for the protection of Electronic Protected Health Information in accordance with 45 CFR Part 164 Subpart C.

III. Third Parties Performing Electronic Data Interchange Transactions

A. Background

45 CFR §162.915, titled "Trading Partner Agreements," states that Trading Partner Agreements cannot contain any provision that adds to or changes the content or meaning of any of the claim types listed in Section IV(2).

B. Applicability

The terms and conditions in this Section III shall apply if Business Associate are transacting any claims of the following types with the Covered Entity:

a) Health care claims or equivalent encounter information
b) Health care payment and remittance advice
c) Coordination of benefits
d) Health care claim status
e) Enrollment and disenrollment in a health plan
f) Eligibility for a health plan
g) Health plan premium payments
h) Referral certification and authorization
i) First report of injury
j) Health claims attachments

C. No changes

Business Associate agree that they will not change the definition, data condition, or use of a data element or segment.

D. No Additions

Business Associate agree not to add any data elements or segments to the maximum defined data set.

E. No Unauthorized Uses

Business Associate agree not to use any code or data elements that are either marked "not used" in the standard's implementation specification or are not in the standard's implementation specifications.

F. No Changes to Meaning or Intent

Business Associate agree to not change the meaning or intent of any of the implementation specifications.

IV. Obligations of Covered Entity

A. ***Provision of Document Templates.*** Covered Entity shall notify Business Associate of any limitation(s) contained in the Notice of Privacy Practices and Authorization Form that the Covered Entity produces in accordance with 45 CFR §164.520 and 45 CFR §164.508, respectively, to the extent that such limitation may affect Business Associate's access, use, or disclosure of PHI.

B. ***Permissions.*** Should an Individual change or revoke permission to use or disclose PHI, Covered Entity shall provide Business Associate with the change, if such change affects Business Associate's permitted or required uses and disclosures.

C. ***Restrictions.*** Covered Entity shall notify Business Associate of any restriction(s) on the use or disclosure of PHI to which the Covered Entity has agreed in conformity with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

D. ***Permissible Requests by Covered Entity*****.** Covered Entity shall not request that Business Associate access, use, or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

E. ***Access and Copies*****.** Covered Entity may send Business Associate any Individual request for access to a copy of that Individual's PHI under 45 CFR §164.524.

F. ***Accounting.*** Covered Entity can request the time frame and manner by which Business Associate may document and make available an accounting of disclosures under 45 CFR §164.528.

G. ***Representations.*** Covered Entity represents and warrants that its Notice of Privacy Practices permits Covered Entity to access, use, and disclose PHI in the manner that Business Associate is authorized to access, use, and disclose PHI under this Agreement and the Underlying Agreement.

V. EFFECTIVE DATE, TERM & TERMINATION

A. ***Effective Date, Term.*** This Agreement is effective as of the effective date in the Underlying Agreement and shall remain in effect until the expiration of the term of the Underlying

Agreement (including any extensions thereof), or until earlier terminated thereunder or hereunder (but only when all the PHI 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 PHI, protections are extended to such information in accordance with the termination provisions herein).

B. ***Termination for Cause.*** If either party believes the other party is in material breach of this Agreement and/or believes it has knowledge of a pattern of activity or practice constituting a material breach or violation of the other party's obligations under this Agreement, that party shall immediately notify the other party in writing and, if such breach is curable, shall provide the other party with an opportunity to take reasonable steps to cure the breach and/or end the violation within thirty (30) days of notification. If the breach is incurable or if the breach is not cured and/or the violation is not ended within the specified time frame, the notifying party may terminate this Agreement. If neither termination nor cure is feasible, the notifying party shall report the violation to the Secretary. Termination of this Agreement shall serve to terminate the Underlying Agreement. These termination rights are in addition to and not in lieu of any termination rights in the Underlying Agreement.

C. ***Effect of Termination.*** Upon termination of this Agreement, for any reason, within 60 days, Business Associate shall return or destroy all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI. Business Associate shall deliver a completed Certificate of Destruction attached hereto as **Exhibit A** of this Agreement. In the event that the parties determine that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity documentation of the conditions that make the return or destruction infeasible. Business Associate shall extend the protections of this Agreement to such PHI and limit further access, use, and disclosure of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. After such time, Business Associate shall deliver a completed Certificate of Destruction to Covered Entity.

VII. MISCELLANEOUS

A. ***Regulatory References.*** A reference in this Agreement, to HIPAA and/or a regulation issued pursuant to HIPAA, means the section as in effect or as amended.

B. ***Survival.*** Any and all obligations of the Covered Entity or Business Associate that are intended to and/or that would naturally survive the expiration or termination of this Agreement shall do so.

C. ***Interpretation and Conflict.*** Any ambiguity in this Agreement shall be resolved to permit compliance with HIPAA. In the event of a conflict between the terms of this Agreement and the terms of the Underlying Agreement, the terms of this Agreement shall prevail with respect to the subject matter herein.

D. ***Entire Agreement, No Third-Party Beneficiaries.*** This Agreement is the entire agreement of the parties with respect to the subject matter herein; supersedes all prior agreements whether in writing or oral; and is not intended to confer on any party, other than the parties hereto, any right, benefit, remedy, or obligation.

Exhibit A. ***Certificate of Destruction***

Organization:	Organization Contact:
Date of Destruction:	Contact Email/Phone:
Description of Information Disposed Of: _____ _____ _____ _____	
Inclusive Dates Covered:	
Method of Destruction: _____ _____ _____ _____	
Records Destroyed By:	
Name:_____ Title:_____ Signature:_____	