HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

TERMS AND CONDITIONS FOR BUSINESS ASSOCIATES

I. Overview / Definitions

The Health Insurance Portability and Accountability Act is a federal law that was enacted on August 21, 1996, and established rules governing the privacy of all identifiable health information regardless of form (referred to as "Protected Health Information" or "PHI"), Electronic Data Interchange (EDI) and Code Set Standards, and the security of PHI. The privacy standards are set forth in the rule entitled "Standards for Privacy of Individually Identifiable Health Information" (the Privacy Rule). The standards established under the Health Insurance Portability and Accountability Act and subsequent interim and supplemental rules were consolidated and further modified by way of the Omnibus Final Rule, which became effective as of March 26, 2013 (collectively referred to herein as "HIPAA"). HIPAA applies to health care providers, health plans, and health care clearinghouses. HIPAA refers to these as "Covered Entities". For purposes of these terms and conditions and HIPAA, a Covered Entity (CE) is the Entity described in the underlying contract to the agreement. HIPAA also indirectly applies to third parties that have access to CE PHI to provide services to, or on behalf of, the CE. HIPAA requires that the CE enter into an agreement with each of these third parties, and that these third parties enter into agreements with their agents and subcontractors that have access to CE PHI, the contents of which is defined by the applicable rule, and is based on the manner and purpose for which CE PHI is being disclosed. Detailed information regarding HIPAA and each of the rules can be found at http://aspe.hhs.gov/admnsimp/.

Terms used herein, but not otherwise defined, shall have the same meaning as those terms in 45 CFR § 160.103, 45 CFR § 164.304, 45 CFR § 164.501 and Pub. L. 111-5 § 13400, as well as defined in Pub. L. 104-191 and Pub. L. 111-5.

II. Third Parties Having Access to Covered Entity's Protected Health Information

1. Background

   45 CFR § 164.502(e), titled "Standards: Disclosures to Business Associates" states that "a covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information… through a written contract or other written agreement or arrangement with the business associate."

2. Applicability
   The terms and conditions in this Section II shall apply if you (as a Business Associate entity as defined in HIPAA and hereinafter referred to as "You" or "Your") have access to CE PHI to provide services to, or on behalf of, CE.

3. Permitted Uses

   a) Except as otherwise limited herein, You may access, use, or disclose CE PHI to perform functions, activities or services for, or on behalf of, CE as specified in an existing contract or arrangement with the CE, provided that such access, use, or disclosure would not violate HIPAA if done by the CE or the minimum necessary policies and procedures of the CE. PHI is defined as individually identifiable information transmitted in any form or medium.

   b) Except as otherwise limited herein, You may access and use CE PHI for Your proper management and administration or to carry out Your legal responsibilities.

   c) Except as otherwise limited herein, You may disclose CE PHI for Your proper management and administration, provided that such disclosures as Required By Law, or if You obtain reasonable assurances from the person to whom the information is disclosed that it will remain confidential and accessed, used, or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notified You of any instances of which it is aware in which the confidentiality of the information has been breached.

   d) Except as otherwise limited herein, You may use CE PHI to provide Data Aggregation services to the CE as permitted by 42 CFR § 164.504(e)(2)(i)(B).

   e) You may use CE PHI to report violations of law to the appropriate federal and state authorities, consistent with 45 CFR § 164.502 (j)(l).

4. Limitation on Access, Use, and Appropriate Safeguards
   You agree to not access, use, or disclose CE PHI other than as permitted or required as provided for herein or as Required By Law. You agree to use appropriate safeguards to prevent such access, use, or disclosure of CE PHI.

5. Report of Breach
   You acknowledge and agree to establish a system to monitor and investigate access, use, and disclosure of CE PHI in accordance with HIPAA. You also agree to take responsibility to investigate any potential inappropriate access, use, or disclosure of

CE PHI under Your control, in order to determine if a reportable breach has occurred under HIPAA. Should You determine that a use or disclosure of CE PHI constituted a reportable breach under HIPAA, You agree to adhere to the reporting requirements under HIPAA. You further agree to immediately report to the CE (1) any access, use, or disclosure of CE PHI not provided for herein of which You become aware, (2) any Security Incident involving the inappropriate disclosure, use, or access of CE PHI of which You become aware, and (3) any breach of Unsecured CE PHI You become aware of as required by Pub. L. 111-5 § 13402(b). Such report shall include the name of each individual whose CE PHI has been, or is reasonably believed by You to have been accessed, acquired, or disclosed during such breach. Such reports shall be submitted within two (2) business days of when You become aware of such breach, and shall contain such information as you reasonably believe is required for the CE to further investigate. You shall also provide such assistance and further information as reasonably requested by the CE. You agree to mitigate, to the extent practicable, any harmful effect that is known to You of an access, use, or disclosure of CE PHI by You in violation of the requirements contained herein.

6. Agent / Subcontractors

   You agree to ensure that any agents, including any subcontractor to whom You provide CE PHI (whether received from or the CE created or received by You) on behalf of the CE, agree to in writing the same restrictions and conditions that apply in these terms to You with respect to such information.

7. Access to Covered Entity's Protected Health Information

   You agree to provide access, at the request of the CE, and in the time and manner as prescribed by HIPAA, to CE PHI in a Designated Record Set, to the CE or, as directed by the CE, to an Individual in order to meet the requirements under 45 CFR § 164.524. Such time and manner shall allow the CE to comply with its obligations under HIPAA.

8. Amendment to Covered Entity's Protected Health Information

   You agree to make any amendment(s) to CE PHI in a Designated Record Set that the CE directs or agrees to pursuant to 45 CFR § 164.526 at the request of the CE or an Individual, and in the time and manner as prescribed by HIPAA. Such time and manner shall allow the CE to comply with its obligations under HIPAA.

9. Accounting of Covered Entity's Protected Health Information

   You agree to document such disclosures of CE PHI and information related to such disclosures as would be required for the CE to respond to a request by an Individual for an accounting of disclosures of CE PHI in accordance with 45 CFR § 164.528

and Pub. L. 111-5 § 13405(c). You further agree to provide to the CE, in a time and manner as prescribed by HIPAA and Pub. L. 111-5, such information collected in accordance with this paragraph in response to a request for an accounting of disclosures of CE PHI in accordance with 45 CFR § 164.528 and Pub. L. 111-5. Such time and manner shall comply with the obligations under HIPAA or Pub. L. 111-5.

10. Property Rights

    The CE PHI shall be and remain the property of the CE. You agree that You acquire no title or rights to the CE PHI, including any de-identified information, as a result of these terms and conditions.

11. Prohibition on Sales of Electronic Health Records or Covered Entity's Protected Health Information

    As required by Pub. L. 111-5 § 13405(d)(1), and unless approved by the CE, consistent with the exceptions set forth in Pub. L. 111-5 § 13405(d)(2), You shall not directly or indirectly receive remuneration in exchange for any CE PHI of an Individual unless the CE has obtained from the Individual a valid authorization that includes a specification of whether the CE PHI can be further exchanged for remuneration by the entity receiving the CE PHI of that Individual.

12. Prohibition on Marketing

    As defined in Pub. L. 111-5 § 13406(a) and 45 CFR § 164.508, and unless approved by the CE, You shall not directly or indirectly perform marketing to CE members using CE PHI that was either provided by the CE or created or otherwise acquired by You on behalf of the CE.

III. Security Standards for the Protection of Electronic Protected Health Information

1. Background

   45 CFR Part 164 Subpart C is titled "Security Standards for the Protection of Electronic Protected Health Information".

2. Applicability

   The terms and conditions in this Section III shall apply if the CE is transmitting Electronic Protected Health Information (EPHI) to You for processing, storage, management, or the like.

3. Security

As required by Pub. L. 111-5 § 13401(a), the following sections of Title 45 of the Code of Federal Regulations ("HIPAA Security Standards") shall also apply to You in Your capacity as a Business Associate:

a) 164.308 (Administrative Safeguards)
b) 164.310 (Physical Safeguards)
c) 164.312 (Technical Safeguards)
d) 164.316 (Policies and Procedures and Documentation Requirements)

These provisions can be found at:

http://www.cms.hhs.gov/SecurityStandard/Download/securityfinalrule.pdf

If You violate any of these provisions, the penalties as set forth in Section 1176 (General Penalty for Failure to Comply with Requirements and Standards) and Section 1177 (Wrongful Disclosure of Individually Identifiable Health Information) of the Social Security Act shall apply to You. This information can be located at:

http://www.ssa.gov/OP_Home/ssact/title11/1176.htm and

http://www.ssa.gov/OP_Home/ssact/title11/1177.htm

4. Property Rights

The EPHI shall be and remain the property of the CE. You agree that You acquire no title or rights to the EPHI, including any de-identified information, as a result of these terms and conditions.

5. Beneficiaries

The individuals who are the subject of the EPHI are intended to be third party beneficiaries of these terms and conditions.

IV. Third Parties Performing Electronic Data Interchange Transactions

1. 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 claims types listed in Section IV(2).

2. Applicability

   The terms and conditions in this Section IV shall apply if You are transacting any claims of the following types with the CE:

   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

3. No Changes

   You agree that You will not change the definition, data condition, or use of a data element or segment in a standard.

4. No Additions

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

5. No Unauthorized Uses

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

6. No Changes to Meaning or Intent

   You agree not to change the meaning or intent of any of the standard's implementation specifications.

7. Property Rights

   The CE PHI shall be and remain the property of the CE. You agree that You acquire no title or rights to the CE PHI, including any de-identified information, as a result of these terms and conditions.

V. General Terms

1. Availability of Books and Records to the Secretary
   You agree to make Your internal practices, books, and records, including policies, procedures, and PHI relating to the access, use, and disclosure of CE PHI received from, or created or received by You on behalf of the CE, available to the Secretary of the United States Department of Health and Human Services (the "Secretary"), in a time and manner as prescribed by HIPAA or designated by the Secretary for purposes of the Secretary determining the CE's compliance with HIPAA. Such time and manner shall allow the CE to comply with its obligations under HIPAA.

2. Subject to Audits by the Secretary
   As provided for in Pub. L. 111-5 Section 13411, You shall be subject to audits by the Secretary to ensure You comply with Subtitle D (Privacy) of Pub. L. 111-5 as well as 45 CFR 164 Subparts C and E.

3. Applicability
   The terms and conditions of this Section V shall apply to You.

4. Term and Termination

   a) These terms and conditions shall terminate when all of the PHI provided by the CE to You, or created or received by You on behalf of the CE, is destroyed or returned to the CE, or if it is not feasible to return or destroy the CE PHI, protections are extended to such information in accordance with the termination provisions in this section.

   b) Termination for Cause – Upon the CE's knowledge of a material breach by You, the CE shall either:

      1) Provide an opportunity for You to cure the breach or end the violation and terminate these terms and conditions if You do not cure the breach or end the violation within the time specified by the CE.

      2) Immediately terminate these terms and conditions if You have breached a material term and cure is not possible, or

      3) If neither termination nor cure is feasible, the CE shall report the violation to the Secretary.

c) Except as provided in paragraph (d) of this section, upon termination of these terms and conditions, for any reason, You shall return or destroy all PHI received from the CE, or created or received by You on behalf of the CE. This provision shall apply to the CE PHI that is in the possession of Your subcontractors or agents. You shall retain no copies of the CE PHI.

d) In the event that You determine that returning or destroying the CE PHI is not feasible, You shall provide to the CE notification of the conditions that make return or destruction not feasible. Upon mutual agreement of the Parties that return or destruction of CE PHI is not feasible, You shall extend the protections of these terms and conditions to such CE PHI and limit further access, uses, and disclosures of such CE PHI to those purposes that make the return or destruction not feasible, for so long as You maintain such CE PHI.

VI. Covered Entity Access to Facilities, Books, and Records

You shall, upon reasonable request, give the CE access for inspection to Your facilities used for the maintenance or processing of CE PHI, and to Your books, records, practices, policies and procedures concerning the access, use, and disclosure of CE PHI, for the purpose of determining Your compliance with these terms and conditions. The CE is also permitted to perform reasonable audits of Your management and use of CE PHI.

1. Covered Entity Obligations

The Covered Entity shall:

a) Provide You with our Notice of Privacy Practices (NOPP) that we produce in accordance with 45 CFR § 164.520. A copy of our NOPP is available at http://www.upmchealthplan.com/privacy.html.

b) Notify You of any limitation(s) in our NOPP in accordance with 45 CFR § 164. 520, to the extent that such limitation(s) may affect Your use or disclosure of CE PHI.

c) Notify You of any changes in, or revocation of, permission by an Individual to use or disclose CE PHI, to the extent that such changes may affect Your use or disclosures of CE PHI.

d) Notify You of any restriction to the access, use, or disclosure of CE PHI that the CE has agreed to in accordance with 45 CFR § 164.522 to the extent that such restriction may affect Your access, use, or disclosure of CE PHI.

e) Not request You access, use, or disclose CE PHI in any manner that would not be permissible under HIPAA if done by the CE, except for Your data aggregation or management and administrative activities and permissible as stipulated herein.

2. Regulatory References
A reference in these terms and conditions to a section in HIPAA means the section as in effect or as amended.

3. Amendment
The Parties agree to take such action as is necessary to amend these terms and conditions, in writing, from time to time as is necessary for the CE to comply with the requirements of HIPAA and HIPAA Pub. L. 104-191.

4. Survival
Your respective rights and obligations under Section 3c and 3d of this section ("Term and Termination") shall survive the termination of these terms and conditions.

5. Interpretation
Any ambiguity in these terms and conditions shall be resolved to permit the CE to comply with HIPAA.

6. Compliance with Laws
You shall take such actions as are necessary for You or the CE to comply with existing or future federal, state, or local statutes, or regulations promulgated by regulatory agencies or accrediting organizations with regards to the services contemplated by this agreement ("Regulations"). You shall perform such work at Your own expense. Such actions will be completed within the times specified for compliance within the statute or regulation. The CE shall have the right at all times to review and inspect the steps taken and procedures implemented by You to assure compliance with such Regulations. In the event that the CE in good faith determines that Your compliance with such Regulations has not or cannot be accomplished by the timeframes required by the Regulation, the CE may terminate this agreement on ninety (90) days prior written notice to You without further liability or penalty.

7. Application of HIPAA Privacy Provisions

As required in Pub. L. 111-5 § 13404, if You know of a pattern of activity or practice that constitutes a material breach or violation of Your obligations under these terms, You must take reasonable steps to cure the breach or end the violation, as applicable. If You are unable to cure the breach or end the violation, You shall inform the CE, and the CE shall either:

a) Terminate the contract or arrangement, if feasible; or
b) Report the problem to the Secretary, if termination is not feasible.

If the Business Associate violates this provision, the penalties as set forth in Section 1176 (General Penalty for Failure to Comply with Requirements and Standards) and Section 1177 (Wrongful Disclosure of Individually Identifiable Health Information) of the Social Security Act shall apply to the Business Associate. These provisions can be found at:
http://www.ssa.gov/OP_Home/ssact/title11/1176.htm and

http://www.ssa.gov/OP_Home/ssact/title11/1177.htm