Health Insurance Portability and Accountability Act (HIPAA) Terms and Conditions For Business Associates

I. OVERVIEW/DEFINITIONS

The Health Insurance Portability and Accountability Act (HIPAA) 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) & 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, the University of Pittsburgh Medical Center (UPMC) and/or subsidiaries are collectively a Covered Entity and referred to herein as UPMC. HIPAA also indirectly applies to third parties that have access to UPMC PHI to provide services to, or on behalf of, UPMC. HIPAA requires that UPMC enter into an agreement with each of these third parties, and that these third parties enter into agreements with their agents and sub-contractors that have access to UPMC PHI, the contents of which is defined by the applicable rule, and is based on the manner and purpose for which the UPMC PHI is being disclosed.

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 § 164.501and 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 UPMC PHI

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 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 UPMC PHI to provide services to, or on behalf of, UPMC.

3. Permitted Uses.

    a) Except as otherwise limited herein, You may use or disclose UPMC PHI to perform functions, activities or services for, or on behalf of, UPMC as specified in an existing contract or arrangement with UPMC, provided that

such use or disclosure would not violate HIPAA, if done by UPMC or the minimum necessary policies and procedures of UPMC. PHI is defined as individually identifiable health information transmitted in any form or medium.

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

c) Except as otherwise limited herein, You may disclose UPMC PHI for Your proper management and administration, provided that such disclosures are Required By Law, or if You obtain 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 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 UPMC PHI to provide Data Aggregation services to UPMC as permitted by 45 CFR §164.504(e)(2)(i)(B).

e) You may use UPMC PHI to report violations of law to the appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1).

4. Limitation on Use and Appropriate Safeguards. You agree to not use or disclose UPMC 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 use or disclosure of UPMC PHI.

5. Report of Breach. You acknowledge and agree to establish a system to monitor and investigate use and disclosure of UPMC PHI in accordance with HIPAA. You also agree to take responsibility to investigate any potential inappropriate access, use, or disclosure of UPMC 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 UPMC PHI constituted a reportable breach under HIPAA, You agree to adhere to the reporting requirements under HIPAA. You further agree to immediately report to UPMC (1) any use or disclosure of UPMC PHI not provided for herein of which you become aware, (2) any Security Incident involving the inappropriate disclosure or access of UPMC PHI of which You become aware, and (3) any breach of Unsecured UPMC PHI You become aware of as required by Pub. L. 111-5 § 13402(b). Such report shall include the name of each individual whose UPMC 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 UPMC to further investigate. You also shall provide such assistance and further information as reasonably requested by UPMC. You agree to mitigate, to the extent practicable, any harmful effect that is known to You of a use or disclosure of UPMC PHI by You in violation of the requirements contained herein.

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

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

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

9. Accounting of UPMC PHI. You agree to document such disclosures of UPMC PHI and information related to such disclosures as would be required for UPMC to respond to a request by an Individual for an accounting of disclosures of UPMC PHI in accordance with 45 CFR § 164.528 and in Pub.L. 111-5 §13405(c). You further agree to provide to UPMC or an Individual, as applicable, 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 UPMC 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. UPMC PHI shall be and remain the property of UPMC. You agree that You acquire no title or rights to UPMC PHI, including any de-identified information, as a result of these terms and conditions.

11. Prohibition on Sale of Electronic Health Records or UPMC PHI. As required by Pub.L. 111-5 §13405(d)(1), and unless approved by UPMC, 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 UPMC PHI of an individual unless UPMC has obtained from the individual a valid authorization that includes a specification of whether the UPMC PHI can be further exchanged for remuneration by the entity receiving the UPMC 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 UPMC, You shall not directly or indirectly perform marketing to UPMC patients using UPMC PHI that was either provided by UPMC or created or otherwise acquired by You on behalf of UPMC.

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 UPMC 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") also shall 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)

   If You violate any of these provisions, the penalties as set forth in Section 1176 (General Penalty For Failure to Comply With Requirements & 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 UPMC. 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.

IV. THIRD PARTIES PERFORMING EDI 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 UPMC:

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

5. No Unauthorized Uses. You agree to not 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 to not change the meaning or intent of any of the standard's implementation specifications.

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

V. GENERAL TERMS

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

2. Availability of Books and Records to Secretary. You agree to make Your internal practices, books, and records, including policies, procedures and PHI relating to the use and disclosure of UPMC PHI received from, or created or received by You on behalf of UPMC, 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 UPMC's compliance with HIPAA. Such time and manner shall allow UPMC to comply with its obligations under HIPAA.

3. UPMC Access to Facilities, Books and Records. You shall, upon reasonable request by UPMC, and with reasonable oversight by You, give UPMC reasonable access for inspection and copying to Your facilities used for the maintenance or processing of UPMC PHI, and to Your books, records, practices, policies, and procedures concerning the use and disclosure of UPMC PHI, for the purpose of determining, in good faith, Your compliance with these terms and conditions. You shall also permit UPMC to perform reasonable audits of Your management and use of UPMC PHI.

4. 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.

5. Term and Termination.

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

   b) Termination for Cause. Upon UPMC's knowledge of a material breach by You, UPMC 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 UPMC.

      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 are feasible, UPMC 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 UPMC, or created or received by You on behalf of UPMC. This provision shall apply to UPMC PHI that is in the possession of Your subcontractors or agents. You shall retain no copies of UPMC PHI.

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

6. UPMC Obligations. UPMC shall:

   a) Provide You with our Notice of Privacy Practices (NOPP) that we produce in accordance with 45 CFR §164.520. For purposes of this obligation, the UPMC NOPP can be accessed at http://purchasing.upmc.com.

b) Notify You of any limitation(s) in our Notice of Privacy Practices in accordance with 45 CFR §164.520, to the extent that such limitation(s) may affect Your use or disclosure of UPMC PHI.

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

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

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

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

8. 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 UPMC to comply with the requirements of HIPAA and HIPAA (Pub.L.No. 104-191).

9. Survival. Your respective rights and obligations under section V(5) parts (c) and (d) ("Term and Termination") shall survive the termination of these terms and conditions.

10. Interpretation. Any ambiguity in these terms and conditions shall be resolved to permit UPMC to comply with HIPAA.

11. Indemnification. You shall defend, indemnify and hold harmless UPMC, and its directors, officers, employees, contractors and agents, from and against any or all cost, losses, expenses, actions, claims, damages, third-party demands, obligations, penalties and liabilities arising out of Your activities or failure to perform Your obligations under this Agreement, except to the extent that such cost, loss, expense, action, claim, damage, third-party demand, obligation, penalty or liability was incurred as a result of the gross negligence or willful misconduct of UPMC. As a condition precedent to Your obligation to indemnify UPMC under this Agreement, UPMC must notify You within a reasonable amount of time upon learning of any cost, loss, expense, action, claim, damage, third-party demand, obligation, penalty or liability in order to give You an opportunity to present any appropriate defense. UPMC shall have the right, but not the obligation, to participate in any defense at its own cost and with its own counsel. The provisions of this paragraph will survive the termination of this Agreement.

12. Compliance with Laws. You shall take such actions as are necessary for You or UPMC 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. UPMC 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 UPMC in good faith determines that Your compliance with such Regulations has not or cannot be accomplished by the timeframes required by the Regulation, UPMC may terminate this agreement on ninety (90) days prior written notice to you without further liability or penalty.

13. 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 UPMC, and UPMC shall either:

a) Terminate the contract or arrangement, if feasible; or

b) If termination is not feasible, report the problem to the Secretary.

If Business Associate violates this provision, the penalties as set forth in Section 1176 (General Penalty for Failure to Comply With Requirements & Standards) and Section 1177 (Wrongful Disclosure of Individually Identifiable Health Information) of the Social Security Act shall apply to 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.

John P. Houston
Vice President, Information Security
and Privacy & Assistant Counsel

James A. Szilagy
Chief Supply Chain Officer

AGREED

CompanyName:

_____

Signature

_____

Name(print)

_____

Title

_____

Date

_____