Policy and Procedure:

# SDM HIPAA Terms and Conditions for Business Associates

(Adapted from UPMC's HIPAA Terms and Conditions for Business Associates at http://www.upmc.com/aboutupmc/supplychainmanagement/Documents/Terms.pdf)

| **Effective:** | 03/30/2012 | **Created:** | 03/21/2012 | **Last updated:** | 5/12/2012 |
|---|---|---|---|---|---|

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

### I. OVERVIEW

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). 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 School of Dental Medicine at the University of Pittsburgh (SDM) and/or subsidiaries are collectively a Covered Entity and referred to herein as SDM. HIPAA also indirectly applies to third parties that have access to SDM's PHI to provide services to, or on behalf of, SDM. HIPAA requires that SDM enter into an agreement with each of these third parties, the contents of which is defined by the applicable rule, and is based on the manner and purpose for which the 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 and § 164.501.

### II. THIRD PARTIES HAVING ACCESS TO 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 or receive 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 the Privacy Rule and hereinafter referred to as "You" or "Your") have access to PHI to provide services to, or on behalf of, SDM.

3. Permitted Uses.

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

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

c) Except as otherwise limited herein, You may disclose 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 PHI to provide Data Aggregation services to SDM as permitted by 42 CFR §164.504(e)(2)(i)(B).

e) You may use 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 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 PHI.

5. Report of Breach. You agree to report to SDM (1) any use or disclosure of PHI not provided for herein of which you become aware of and (2) any Security Incident involving the inappropriate disclosure or access of PHI of which You become aware of. 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 SDM to further investigate. You shall also provide such assistance and further information as reasonably requested by SDM. You agree to mitigate, to the extent practicable, any harmful effect that is known to You of a use or disclosure of 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 PHI (whether received from or created or received by You) on behalf of SDM agree to the same restrictions and conditions that apply in these terms to You with respect to such information.

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

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

9. Accounting of PHI. You agree to document such disclosures of PHI and information related to such disclosures as would be required for SDM to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. You further agree to provide to SDM or an Individual, in a time and manner as prescribed by the Privacy Rule, such information collected in accordance with this paragraph to permit SDM to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Such time and manner shall allow SDM to comply with its obligations under the Privacy Rule.

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

## III. SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

1. Background. 45 CFR § 164.314 titled "Organizational Requirements" identifies required security related business associate terms and conditions.

2. Applicability. The terms and conditions in this Section III shall apply if SDM is transmitting electronic protected health information (EPHI) to You for processing, storage, management or the like.

3. Security. You shall:

    a) Implement administrative, technical and physical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the EPHI that it creates, receives, maintains or transmits on behalf of SDM

    b) Ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate safeguards to protect it.

4. Property Rights. The EPHI shall be and remain the property of SDM. 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 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 SDM:

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

## V. GENERAL TERMS

1. 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 PHI received from, or created or received by You on behalf of SDM available to the Secretary of the United States Department of Health and Human Services (the "Secretary"), in a time and manner as prescribed by the Privacy Rule or designated by the Secretary for purposes of the Secretary determining SDM's compliance with the Privacy Rule. Such time and manner shall allow SDM to comply with its obligations under the Privacy Rule.

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

3. Term and Termination.

a) These terms and conditions shall terminate (a) when all of the PHI provided by SDM to You, or created or received by You on behalf of SDM, is destroyed or returned to

SDM, or, if it is not feasible to return or destroy the PHI, protections are extended to such information, in accordance with the termination provisions in this section.

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

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

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

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

5. SDM Obligations. SDM 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 SDM 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 PHI.

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

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

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

6. Regulatory References. A reference in these terms and conditions to a section in the Privacy Rule means the section as in effect or as amended.

7. 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 SDM to comply with the requirements of the Privacy Rule and HIPAA (Pub.L.No. 104-191).

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

9. Interpretation. Any ambiguity in these terms and conditions shall be resolved to permit SDM to comply with the Privacy Rule.

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