

## **Business Associate Agreement**

### **1. PREAMBLE AND DEFINITIONS.**

- 1.1. Pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended (“**HIPAA**”), \_\_\_\_\_ (“**Covered Entity**”) and MedPharm Services LLC or any of its corporate affiliates (“**Business Associate**”), a Puerto Rico limited liability company, enter into this Business Associate Agreement (“**BAA**”) as of \_\_\_\_\_ (the “**Effective Date**”) that addresses the HIPAA requirements with respect to “business associates,” as defined under the privacy, security, breach notification, and enforcement rules at 45 C.F.R. Part 160 and Part 164 (“**HIPAA Rules**”). A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended.
- 1.2. This BAA is intended to ensure that Business Associate will establish and implement appropriate safeguards for the Protected Health Information (“**PHI**”) (as defined under the HIPAA Rules) that Business Associate may receive, create, maintain, use, or disclose in connection with the functions, activities, and services that Business Associate performs for Covered Entity. The functions, activities, and services that Business Associate performs for Covered Entity are defined in the End User License Agreement.
- 1.3. Pursuant to changes required under the Health Information Technology for Economic and Clinical Health Act of 2009 (the “**HITECH Act**”) and under the American Recovery and Reinvestment Act of 2009 (“**ARRA**”), this BAA also reflects federal breach notification requirements imposed on Business Associate when “Unsecured PHI” (as defined under the HIPAA Rules) is acquired by an unauthorized party and the expanded privacy and security provisions imposed on business associates.
- 1.4. Unless the context clearly indicates otherwise, the following terms in this BAA shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, disclosure, Electronic Media, Electronic Protected Health Information (ePHI), Health Care Operations, individual, Minimum Necessary, Notice of Privacy Practices, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured PHI, and use.
- 1.5. A reference in this BAA to the Privacy Rule means the Privacy Rule, in conformity with the regulations at 45 C.F.R. Parts 160-164 (the “**Privacy Rule**”) as interpreted under applicable regulations and guidance of general application published by HHS, including all amendments thereto for which compliance is required, as amended by the HITECH Act, ARRA, and the HIPAA Rules.

### **2. GENERAL OBLIGATIONS OF BUSINESS ASSOCIATE.**

- 2.1. Business Associate agrees not to use or disclose PHI, other than as permitted or required by this BAA or as Required by Law, or if such use or disclosure does not otherwise cause a Breach of Unsecured PHI.
- 2.2. Business Associate agrees to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to ePHI to prevent use or disclosure of PHI other than as provided for by the BAA.
- 2.3. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate as a result of a use or disclosure of PHI by Business Associate in violation of this BAA’s requirements or that would otherwise cause a Breach of Unsecured PHI.
- 2.4. The Business Associate agrees to the following breach notification requirements:
  - 2.4.1. Business Associate agrees to report to Covered Entity any Breach of Unsecured PHI not provided for by the BAA of which it becomes aware within sixty (60) calendar days of “discovery” within the meaning of the HITECH Act. Such notice shall include the identification of each individual whose Unsecured PHI has been or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed in connection with such Breach. In addition, Business Associate shall provide any additional information reasonably requested by Covered Entity for purposes of investigating the Breach and any other available information that Covered Entity is required to include to the individual under 45 C.F.R. § 164.404(c) at the time of notification or promptly thereafter as information becomes available. Business Associate’s notification of a Breach of Unsecured PHI under this Section shall comply in all respects with each applicable provision of Section 13400 of Subtitle D (Privacy) of ARRA, the HIPAA Rules, and related guidance issued by the Secretary or the delegate of the Secretary from time to time.
  - 2.4.2. In the event of Business Associate’s use or disclosure of Unsecured PHI in violation of HIPAA, the

HITECH Act, or ARRA, Business Associate bears the burden of demonstrating that notice as required under this Section 2.4 was made, including evidence demonstrating the necessity of any delay, or that the use or disclosure did not constitute a Breach of Unsecured PHI.

- 2.5. Business Associate agrees, in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, to require that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.
- 2.6. Business Associate agrees to make available PHI in a Designated Record Set to the Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524.
  - 2.6.1. Business Associate agrees to comply with an individual's request to restrict the disclosure of their personal PHI in a manner consistent with 45 C.F.R. § 164.522, except where such use, disclosure, or request is required or permitted under applicable law.
  - 2.6.2. Business Associate agrees that when requesting, using, or disclosing PHI in accordance with 45 C.F.R. § 164.502(b)(1) that such request, use, or disclosure shall be to the minimum extent necessary, including the use of a "limited data set" as defined in 45 C.F.R. § 164.514(e)(2), to accomplish the intended purpose of such request, use, or disclosure, as interpreted under related guidance issued by the Secretary from time to time.
- 2.7. Business Associate agrees to make any amendments to PHI in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 C.F.R. § 164.526 or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526.
- 2.8. Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.528.
- 2.9. Business Associate agrees to make its internal practices, books, and records, including policies and procedures regarding PHI, relating to the use and disclosure of PHI and Breach of any Unsecured PHI received from Covered Entity, or created or received by the Business Associate on behalf of Covered Entity, available to Covered Entity (or the Secretary) for the purpose of Covered Entity or the Secretary determining compliance with the Privacy Rule (as defined in Section 8).
- 2.10. To the extent that Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Business Associate agrees to comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).
- 2.11. Business Associate agrees to account for the following disclosures:
  - 2.11.1. Business Associate agrees to maintain and document disclosures of PHI and Breaches of Unsecured PHI and any information relating to the disclosure of PHI and Breach of Unsecured PHI in a manner as would be required for Covered Entity to respond to a request by an individual or the Secretary for an accounting of PHI disclosures and Breaches of Unsecured PHI.
  - 2.11.2. Business Associate agrees to provide to Covered Entity, or to an individual at Covered Entity's request, information collected in accordance with this Section 2.11, to permit Covered Entity to respond to a request by an individual or the Secretary for an accounting of PHI disclosures and Breaches of Unsecured PHI.
  - 2.11.3. Business Associate agrees to account for any disclosure of PHI used or maintained as an Electronic Health Record (as defined in Section 5) ("**EHR**") in a manner consistent with 45 C.F.R. § 164.528 and related guidance issued by the Secretary from time to time; provided that an individual shall have the right to receive an accounting of disclosures of EHR by the Business Associate made on behalf of the Covered Entity only during the three years prior to the date on which the accounting is requested whether from Covered Entity or directly from the Business Associate.
  - 2.11.4. In the case of an EHR that the Business Associate acquired on behalf of the Covered Entity as of January 1, 2009, paragraph 2.11.3 above shall apply to disclosures with respect to PHI made by the Business Associate from such EHR on or after January 1, 2014. In the case of an EHR that the Business

Associate acquires on behalf of the Covered Entity after January 1, 2009, paragraph 2.11.3 above shall apply to disclosures with respect to PHI made by the Business Associate from such EHR on or after the later of January 1, 2011, or the date that it acquires the EHR.

- 2.12. Business Associate agrees to comply with the "Prohibition on Sale of Electronic Health Records or Protected Health Information," as provided in Section 13405(d) of Subtitle D (Privacy) of ARRA, and the "Conditions on Certain Contacts as Part of Health Care Operations," as provided in Section 13406 of Subtitle D (Privacy) of ARRA and related guidance issued by the Secretary from time to time.
- 2.13. Business Associate acknowledges that, effective on the Effective Date of this BAA, it shall be liable under the civil and criminal enforcement provisions set forth at 42 U.S.C. § 1320d-5 and 1320d-6, as amended, for failure to comply with any of the use and disclosure requirements of this BAA and any guidance issued by the Secretary from time to time with respect to such use and disclosure requirements.

### **3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.**

- 3.1. General Uses and Disclosures. Business Associate agrees to receive, create, use, or disclose PHI only in a manner that is consistent with this BAA, the Privacy Rule, or Security Rule (as defined in Section 5) and only in connection with providing services to Covered Entity; provided that the use or disclosure would not violate the Privacy Rule, including 45 C.F.R. § 164.504(e), if the use or disclosure would be done by Covered Entity. For example, the use and disclosure of PHI will be permitted for "treatment, payment, and health care operations," in accordance with the Privacy Rule.
- 3.2. Business Associate may use or disclose PHI as Required By Law.
- 3.3. Business Associate agrees to make uses and disclosures and requests for PHI consistent with Covered Entity's Minimum Necessary policies and procedures, which shall be provided by Covered Entity in a prompt manner following the Effective Date of the BAA.
- 3.4. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity.
- 3.5. Specific Other Uses and Disclosures:
  - 3.5.1. Except as otherwise limited in this BAA, Business Associate may use PHI to provide Data Aggregation Services to Covered Entity as permitted by HIPAA.
  - 3.5.2. Except as otherwise provided in this BAA, Business Associate may use PHI for its proper management and administration or carry out its legal responsibilities as permitted under applicable law.
  - 3.5.3. Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI of an individual without Covered Entity's prior written approval and notice from Covered Entity that it has obtained from the individual, in accordance with 45 C.F.R. § 164.508, a valid authorization that includes a specification of whether the PHI can be further exchanged for remuneration by Business Associate. The foregoing shall not apply to Covered Entity's payments to Business Associate for services delivered by Business Associate to Covered Entity.
  - 3.5.4. Business Associate may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).
  - 3.5.5. Business Associate may use PHI for Marketing purposes in accordance to 45 CFR § 164.501 and 164.508(a)(3) following the due diligences for such use.

### **4. OBLIGATIONS OF COVERED ENTITY.**

- 4.1. Covered Entity shall:
  - 4.1.1. Provide Business Associate with the Notice of Privacy Practices that Covered Entity produces in accordance with the Privacy Rule, and any changes or limitations to such notice under 45 C.F.R. § 164.520, to the extent that such changes or limitations may affect Business Associate's use or disclosure of PHI.

- 4.1.2. Notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI under this BAA.
- 4.1.3. Notify Business Associate of any changes in or revocation of permission by an individual to use or disclose PHI, if such change or revocation may affect Business Associate's permitted or required uses and disclosures of PHI under this BAA.
- 4.2. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy and Security Rule if done by Covered Entity, except as provided under Section 3 of this BAA.

5. **COMPLIANCE WITH SECURITY RULE.**

- 5.1. Effective April 20, 2005, Business Associate shall comply with the HIPAA Security Rule, which shall mean the Standards for Security of Electronic Protected Health Information at 45 C.F.R. Part 160 and Subparts A and C of Part 164, as amended by ARRA and the HITECH Act. The term "**Electronic Health Record**" or "**EHR**" as used in this BAA shall mean an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.
- 5.2. In accordance with the Security Rule, Business Associate agrees to:
  - 5.2.1. Implement the administrative safeguards set forth at 45 C.F.R. § 164.308, the physical safeguards set forth at 45 C.F.R. § 164.310, the technical safeguards set forth at 45 C.F.R. § 164.312, and the policies and procedures set forth at 45 C.F.R. § 164.316, to reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the Security Rule. Business Associate acknowledges that, effective on the Effective Date of this BAA, (a) the foregoing safeguards, policies, and procedures requirements shall apply to Business Associate in the same manner that such requirements apply to Covered Entity, and (b) Business Associate shall be liable under the civil and criminal enforcement provisions set forth at 42 U.S.C. § 1320d-5 and 1320d-6, as amended from time to time, for failure to comply with the safeguards, policies, and procedures requirements and any guidance issued by the Secretary from time to time with respect to such requirements;
  - 5.2.2. Require that any agent, including a Subcontractor, to whom it provides such PHI agrees to implement reasonable and appropriate safeguards to protect the PHI; and
  - 5.2.3. Report to the Covered Entity any Security Incident of which it becomes aware.

6. **INDEMNIFICATION; LIMITATION OF LIABILITY.**

- 6.1. Business Associate shall indemnify, defend, and hold harmless the Covered Entity, and Covered Entity's affiliates ("Indemnified Parties"), from and against any and all losses, expense, damage, or injury (including, without limitation, all costs and reasonable attorneys' fees) that the Indemnified Parties may sustain as a result of, or arising out of (a) a breach of this BAA by Business Associate or its agents or Subcontractors, including but not limited to any unauthorized use, disclosure, or breach of PHI, (b) Business Associate's failure to notify any and all parties required to receive notification of any Breach of Unsecured PHI pursuant to Section 2.4, or (c) any negligence or wrongful acts or omissions by Business Associate or its agents or Subcontractors, including without limitations, failure to perform Business Associate's obligations under this BAA, the Privacy Rule, or the Security Rule. Notwithstanding the foregoing, nothing in this Section shall limit any rights any of the Indemnified Parties may have to additional remedies under the Underlying Agreement or under applicable law for any acts or omissions of Business Associate or its agents or Subcontractors.
- 6.2. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED HEREIN, NEITHER PARTY WILL BE LIABLE TO THE OTHER UNDER THIS BAA FOR CONSEQUENTIAL, INCIDENTAL, PUNITIVE, SPECIAL, EXEMPLARY OR INDIRECT DAMAGES, OR LOST PROFITS IN CONNECTION WITH CLAIMS MADE BY ANY PARTY, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR TORT. EACH PARTY'S MAXIMUM AGGREGATE LIABILITY TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY LOSSES, DAMAGES OR OTHER LIABILITIES, WHETHER BASED ON WARRANTY, CONTRACT, NEGLIGENCE, OR OTHERWISE, WILL NOT EXCEED THE SUM OF ALL FEES PAID BY CLIENT TO BUSINESS ASSOCIATE DURING THE TWELVE (12) MONTH PERIOD PRIOR TO THE OCCURRENCE OF THE EVENT(S) GIVING RISE TO THE CLAIM. THE FOREGOING LIMITATION OF LIABILITY SHALL

APPLY REGARDLESS OF THE CAUSE OF ACTION ASSERTED BY CLIENT OR ANY THIRD PARTY IN ANY JURISDICTION IN WHICH THE FOREGOING LIMITATION OF LIABILITY IS RESTRICTED. BUSINESS ASSOCIATE'S LIABILITY SHALL BE LIMITED TO THE GREATEST EXTENT PERMITTED BY LAW. THE PROVISIONS OF THIS SECTION SHALL SURVIVE TERMINATION OF THIS AGREEMENT FOR ANY REASON.

## **7. TERM AND TERMINATION.**

- 7.1. This BAA shall be in effect as of the Effective Date above and shall terminate on the earlier of the date that:
  - 7.1.1. Either party terminates the Underlying Agreement.
  - 7.1.2. Either party terminates the BAA for cause as authorized under Section 7.2.
  - 7.1.3. All of the PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity. If it is not feasible to return or destroy PHI, protections are extended in accordance with Section 7.3.
- 7.2. Upon either party's knowledge of a material breach by the other party, the non-breaching party shall provide an opportunity for the breaching party to cure the breach or end the violation; or terminate the BAA. If the breaching party does not cure the breach or end the violation within a reasonable timeframe not to exceed thirty (30) days from the notification of the breach, or if a material term of the BAA has been breached, and a cure is not possible, the non-breaching party may terminate this BAA and the Underlying Agreement, upon written notice to the other party.
- 7.3. Upon termination of this BAA for any reason, the parties agree that Business associate shall return to Covered Entity or, if agreed to by Covered Entity, destroy all PHI received from Covered Entity or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. The PHI shall be returned in a format that is reasonably expected to preserve its accessibility and usability. Business Associate shall retain no copies of the PHI.
- 7.4. The obligations of Business Associate under this Section 7 shall survive the termination of this BAA.

## **8. MISCELLANEOUS.**

- 8.1. This BAA shall automatically incorporate any change or modification as of the effective date of the change or modification to comply with the requirements of the Privacy Rule, the Security Rule, HIPAA, ARRA, the HITECH Act, the HIPAA Rules, and any other applicable law. The Business Associate agrees to maintain compliance with all changes or modifications.
- 8.2. The respective rights and obligations of Business Associate under Section 6 and Section 7 of this BAA shall survive the termination of this BAA.
- 8.3. This BAA shall be interpreted in the following manner:
  - 8.3.1. Any ambiguity shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Rules.
  - 8.3.2. Any inconsistency between the BAA's provisions and the HIPAA Rules, including all amendments, as interpreted by the HHS, a court, or another regulatory agency with authority over the Parties, shall be interpreted according to the interpretation of the HHS, the court, or the regulatory agency.
  - 8.3.3. Any provision of this BAA that differs from those required by the HIPAA Rules, but is nonetheless permitted by the HIPAA Rules, shall be adhered to as stated in this BAA.
- 8.4. This BAA constitutes the entire agreement between the parties related to the subject matter of this BAA, except to the extent that the [UNDERLYING AGREEMENT] imposes more stringent requirements related to the use and protection of PHI upon Business Associate. This BAA supersedes all prior negotiations, discussions, representations, or proposals, whether oral or written. This BAA may not be modified unless done so in writing and signed by a duly authorized representative of both parties. If any provision of this BAA, or part thereof, is found to be invalid, the remaining provisions shall remain in effect.

- 8.5. This BAA will be binding on the successors and assigns of the Covered Entity and the Business Associate. However, this BAA may not be assigned, in whole or in part, without the written consent of the other party. Any attempted assignment in violation of this provision shall be null and void.
- 8.6. This BAA may be executed in two or more counterparts, each of which shall be deemed an original.
- 8.7. Except to the extent preempted by federal law, this BAA shall be governed by and construed in accordance with the same internal laws as that of the Underlying Agreement.

IN WITNESS WHEREOF, the parties hereto have executed this BAA as of the date first above written.

**BUSINESS ASSOCIATE**

**COVERED ENTITY**

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

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

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_