

### Subcontractor Business Associate Agreement

This Business Associate Agreement (this “**Agreement**”) is entered into, and supplements and is made a part of the Services Agreement (the “**Services Agreement**”) by and between Physicians Insurance Risk Retention Group, Inc., a Vermont captive insurance company, serviced by its affiliate Physicians Insurance Member Services, LLC (collectively known as the “**Business Associate**”), and its subcontractor or vendor (the “**Subcontractor**”). This Agreement sets forth the Subcontractor’s responsibilities and obligations for the services provided to the Business Associate under the Services Agreement with respect to the Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health Act (“**HITECH**”) and regulations promulgated thereunder, as such law and regulations may be amended from time to time (collectively, “**HIPAA**”).

### BACKGROUND

A. The Business Associate provides various services to health care providers known as covered entities (the “**Covered Entity**”) under separate agreements between the Business Associate and the Covered Entity (the “**Underlying Agreements**”).

B. Under the Underlying Agreements, the Covered Entity may make available and/or disclose to the Business Associate certain individually identifiable Protected Health Information (“**PHI**”) relating to patients of the Covered Entity that is subject to protection under HIPAA, and the Business Associate agrees to only use or disclose such PHI in accordance with the separately required business associate agreements entered into with each Covered Entity (“**Additional BAA**”).

C. The Subcontractor shall provide services (the “**Services**”) to the Business Associate in order for the Business Associate to perform its responsibilities and obligations to the Covered Entity under each Underlying Agreement and Additional BAA. The Subcontractor is a “business associate” of the Business Associate as defined in 45 CFR § 160.103.

D. HIPAA requires Business Associate to obtain, and Subcontractor to provide, satisfactory written assurances before Subcontractor may create, receive, maintain, or Disclose PHI to perform Services by Subcontractor. This Agreement is entered into to provide the written assurances required under HIPAA.

The parties agree as follows:

### AGREEMENT

**1. DEFINITIONS.** Unless otherwise defined in this Agreement, capitalized terms shall have the same meanings as set forth in HIPAA under 45 CFR Parts 160 and 164 as amended or supplemented from time to time.

## **2. PERMITTED USES AND DISCLOSURES BY THE SUBCONTRACTOR.**

2.1 Permitted Uses. The Subcontractor will use or disclose PHI received from the Business Associate or a Covered Entity only for those purposes necessary to perform the Services, or as otherwise expressly permitted in this Agreement, provided that such use or disclosure would not violate HIPAA.

2.2 Proper Management and Administration. The Subcontractor shall not use or further disclose PHI other than as permitted or required by the Services Agreement, this Agreement, or as required by law. In using, disclosing, or requesting PHI from the Business Associate, the Subcontractor agrees to limit PHI to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request. "Minimum necessary" shall be interpreted in accordance with the HITECH Act and the HIPAA Rules, and implementing regulation or guidance on the definition.

2.3 Data Aggregation. The Subcontractor may use PHI to perform data aggregation services as permitted by 45 CFR § 164.504(e)(2)(i)(B).

2.4 Use by or Disclosure to the Subcontractor or Agent. The Subcontractor agrees that if it provides PHI to a subcontractor or agent to perform the Services for the Business Associate or a Covered Entity, the Subcontractor will first enter into a written agreement with such subcontractor or agent that contains the same terms, conditions, and restrictions on the use and disclosure of PHI as contained in this Agreement in accordance with 45 CFR § 164.502(e)(1)(ii). If the Subcontractor becomes aware of a pattern or practice of activity of a subcontractor or agent that would constitute a material Breach or violation of the written agreement between the Subcontractor and such subcontractor or agent, the Subcontractor shall take reasonable steps to cure such Breach or terminate such written agreement with such subcontractor or agent.

2.5 Independent Contractors. In the performance of the duties and obligations of the parties pursuant to this Agreement, each of the parties shall at all times be acting and performing as an independent contractor, and nothing in this Agreement shall be construed or deemed to create a relationship of employer and employee, or partner, or joint venture, or principal and agent between the parties.

## **3. OBLIGATIONS AND ACTIVITIES OF THE SUBCONTRACTOR.**

3.1 Safeguards. The Subcontractor shall use appropriate safeguards, including without limitation, administrative, physical and technical safeguards, to prevent the use or disclosure of the PHI other than as provided for by this Agreement and to reasonably and appropriately employ the same standards as required by law to, protect the confidentiality, integrity and availability of any PHI that it may receive, maintain or transmit on behalf of the Business Associate or Covered Entity.

3.2 Mitigation. The Subcontractor shall mitigate or cure, to the extent practicable, any harmful effect that is known to the Subcontractor as a result of the Subcontractor's use or disclosure of PHI which violates any requirement of this Agreement.

3.3 Request for Access to PHI. Within four (4) business days of a request by the Business Associate or a Covered Entity for access to PHI, the Subcontractor shall make requested PHI available to the Business Associate or such Covered Entity as required under 45 CFR § 164.524.

3.4 Request for Access to PHI by Individual. If the Subcontractor receives a request from an individual or an individual's designee for PHI, the Subcontractor shall forward any such request to the Business Associate and/or Covered Entity within ten (10) business days and will coordinate any responsive communication to the request as directed by the Business Associate and/or a Covered Entity.

3.5 Amending PHI. The Subcontractor shall make any amendment(s) to PHI in a Designated Record Set (as defined in 45 CFR § 164.501) as the Business Associate or a Covered Entity may direct or agree to pursuant to 45 CFR § 164.526 based upon a written request made by a Covered Entity or an individual. If the Subcontractor receives a request from an individual or an individual's designee to amend PHI in a Designated Record Set, the Subcontractor will forward any such request to the Business Associate within four (4) business days and will coordinate any responsive communication to the requested amendment as directed by the Covered Entity and/or Business Associate.

3.6 Internal Practices, Books and Records. The Subcontractor shall make its internal practices, books and records relating to the use or disclosure of PHI available to the Secretary of the Department of Health and Human Services (the "**Secretary**") or state regulatory body in a time and manner designated by the Secretary or state regulatory body for purposes of determining compliance with HIPAA and/or applicable state law. Notwithstanding this provision, no attorney-client, accountant-client or other legal privilege will be deemed waived by the Subcontractor or the Business Associate as a result of this Agreement.

3.7 Accounting of PHI Disclosure.

(a) The Subcontractor shall document and keep a record of any disclosure of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance 45 CFR § 164.528.

(b) The Subcontractor shall provide the Business Associate, an applicable Covered Entity or an individual with information collected in accordance with subparagraph (a) of this Section 3.7 to permit the Business Associate and such Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

(c) The Subcontractor shall maintain this disclosure record for six (6) years from the termination of this Agreement.

3.8 Notifications Regarding Breaches of Unsecured PHI.

(a) Reporting of Unauthorized Use and Disclosure of PHI. The Subcontractor shall provide a report to Business Associate of any uses or disclosures of PHI not authorized by the Services Agreement or this Agreement of which it becomes aware not more than three (3) calendar days after the unauthorized use or disclosure is discovered.

(b) Reporting of Breach of Unsecured Protected Health Information. Unless state law requires a shorter notification period, the Subcontractor shall notify Business Associate within three (3) calendar days following the discovery of a suspected or actual Breach of Unsecured Protected Health Information ("**Unsecured PHI**"). A suspected or actual Breach shall be treated as discovered by

Subcontractor as of the first day on which the Breach is known to the Subcontractor. If a delay is requested by a law enforcement official in accordance with 45 CFR § 164.412, the Subcontractor may delay notifying Business Associate for the applicable period of time.

(c) Content of Notice. The notice of unauthorized use or disclosure, or of Breach of Unsecured PHI, shall include:

i. To the extent possible, the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Subcontractor to have been improperly accessed, acquired, used or disclosed;

ii. The nature of the Breach or other non-permitted use or disclosure, including a brief description of what happened, the date of the non-permitted use or disclosure or Breach and the date of discovery;

iii. A description of the types of Unsecured PHI that were involved in the non-permitted use or disclosure or Breach, including the types of identifiers;

iv. Such other information as the Business Associate may reasonably request.

(d) Security Incidents. The Subcontractor will report to Business Associate any attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI provided by Business Associate or interference with the Subcontractor's system operations in the Subcontractor's information system of which the Subcontractor becomes aware. The parties acknowledge that probes and reconnaissance scans are commonplace in the industry and, as such, the parties acknowledge and agree that, to the extent such probes and reconnaissance scans constitute Security Incidents, this Section 3.8(d) constitutes notice by the Subcontractor to Business Associate of the ongoing existence and occurrence of such Security Incidents for which no additional notice to Business Associate shall be required, as long as such probes and reconnaissance scans do not result in unauthorized access, use, or disclosure of PHI. Probes and reconnaissance scans include, without limitation, pings and other broadcast attacks on the Subcontractor's firewall, port scans, and unsuccessful log-on attempts that do not result in unauthorized access, use, or disclosure of PHI.

(e) State Law Requirements. In the event the Subcontractor has an independent notification obligation related to impermissible use or disclosure of PHI in connection with this Agreement or the Services Agreement, the Subcontractor shall promptly notify Business Associate of such obligation and, at least two (2) business days before giving any such notice, the Subcontractor shall notify Business Associate of its intent to provide the required notifications, including any related information required by applicable state law.

(f) The Subcontractor shall establish reasonable systems to detect Breaches of Unsecured PHI and provide appropriate training to its workforce members, if applicable, regarding the Subcontractor's policies and procedures pertaining to use and disclosure of PHI and the detection and reporting of Breaches of Unsecured PHI.

3.9 Prohibition on Sale of PHI. Except as otherwise expressly permitted by the HIPAA Rules, the Subcontractor shall not directly or indirectly receive remuneration, including financial or

nonfinancial remuneration, in exchange for an Individual's PHI unless the Covered Entity, Business Associate or the Subcontractor obtains a valid authorization that meets the requirements of 45 CFR § 164.508 and states that the disclosure will result in remuneration to the Covered Entity, Business Associate, or the Subcontractor.

#### **4. OBLIGATIONS OF THE BUSINESS ASSOCIATE.**

4.1 Notification of Restrictions. The Business Associate shall promptly notify the Subcontractor in writing of any restrictions on the use or disclosure of an individual's PHI that the Business Associate or Covered Entity has agreed to, or is required to, abide by under 45 CFR § 164.522, to the extent that such restriction may reasonably affect the Subcontractor's use or disclosure of PHI.

4.2 Notification of Privacy Practices. The Business Associate shall promptly notify the Subcontractor of any limitations in the form or notice of privacy practices that the Business Associate or Covered Entity provides to individuals pursuant to 45 CFR § 164.520, to the extent that such limitation may affect the Subcontractor's use or disclosure of PHI.

#### **5. TERM AND TERMINATION.**

5.1 Term. This Agreement is effective as of the date of execution of the Services Agreement and shall terminate on the earlier date of either the (i) termination of the Services Agreement, or (ii) termination of this Agreement in accordance with Section 5.2.

5.2 Termination for Cause. Without limiting the rights of the parties set forth elsewhere in this Agreement or the Services Agreement or available under applicable law, if either party Breaches its material obligations under this Agreement, then the Breaching party shall promptly take reasonable steps to cure the violation as may be mutually agreed upon with the non-Breaching party to maintain compliance with this Agreement and the non-Breaching party shall retain the right to report the violation to the Secretary. The Breaching party shall have thirty (30) days to cure the violation, if curable. If the Breaching party has not cured the Breach within thirty (30) days to the reasonable satisfaction of the non-Breaching party, or if cure of the Breach is not reasonably possible, the non-Breaching party may immediately terminate this Agreement.

5.3 Effect of Termination. Upon termination, cancellation, expiration or other conclusion of this Agreement, the Subcontractor will limit its further use or disclosure of PHI to those purposes that make return or destruction of PHI infeasible. The Subcontractor will provide notice of those purposes that make return or destruction of PHI infeasible. The Subcontractor will continue to protect the security of any PHI that is maintained pursuant to the security provisions of this Agreement for so long as PHI is maintained.

#### **6. MISCELLANEOUS.**

6.1 Compliance with and Changes to Laws. The parties are required to comply with applicable federal and state laws. If HIPAA is amended or if new laws and/or regulations affecting the terms of this Agreement are required, the parties shall engage in good faith negotiations to amend the terms of this Agreement in accordance with the new amendments, laws and/or regulations. If the parties are unable to agree on such modifications following a reasonable period of good faith negotiations, then

any party that would become noncompliant in the absence of such modifications shall have the right to terminate this Agreement and the Services Agreement and the provisions of Section 5.3 shall then apply.

6.2 Interpretation. Any ambiguity in this Agreement shall be resolved to permit compliance by the parties with HIPAA and any applicable state law.

6.3 No Third Party Beneficiaries. Nothing in this Agreement will confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

6.4 Governing Law. This Agreement shall be interpreted, enforced, and governed in accordance with the laws of the State of Washington, notwithstanding any conflict of law doctrine to the contrary.

6.5 Disputes. If any controversy, dispute, or claim arises between the parties with respect to this Agreement, the parties shall make good faith efforts to resolve such matters informally and in accordance with the dispute resolution process specified in the Services Agreement

6.6 Survival. The Subcontractor's obligations to protect the privacy and safeguard the security of PHI as set forth in this Agreement shall survive the termination of this Agreement.

6.7 Notices. Notices to be given to any of the parties shall be in writing and either hand delivered or sent by registered or certified mail, return receipt requested, or by established one day courier services and postage prepaid to the addresses that may be furnished or updated from time to time be each party.

6.8 Entire Agreement. This Agreement constitutes the entire agreement between the parties with regard to HIPAA and its Privacy Standards and Security Standards. There are no understandings or agreements relating to this Agreement that are not fully expressed in this Agreement.

6.9 Incorporation into the Services Agreement. This Agreement shall be considered an attachment to the Services Agreement and incorporated as though fully set forth within the Services Agreement. This Agreement will govern in the event of conflict or inconsistency with any provision of the Services Agreement.