PHYSICIANS INSURANCE RRG

Business Associate Agreement

This Agreement replaces all prior Business Associate Agreements with Physicians Insurance Risk Retention Group, Inc., a Vermont captive insurance company, serviced by its affiliate Physicians Insurance Member Services, LLC (collectively referred to as "Physicians Insurance RRG").

WHEREAS Physicians Insurance RRG is a "Business Associate" of certain covered entities (the "Covered Entity") under the Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and the regulations implementing Subtitle D of the Health Information Technology for Economic and Clinical Health Act which is Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5) (together "HIPAA"); and Physicians Insurance RRG receives, uses and/or discloses, and maintains "Protected Health Information" ("PHI") (as defined in the aforementioned laws and regulations) in order to perform services under insurance policies or under other types of contracts (together "Services Agreement"); and Physicians Insurance RRG's insureds and other customers who disclose PHI to Physicians Insurance RRG are Covered Entities under the aforementioned laws and regulations who must enter into written contracts with their Business Associates in order to assure certain protections for the privacy and security of PHI; the purpose of this Agreement is to satisfy certain standards and requirements of HIPAA in terms of handling PHI. Physicians Insurance RRG agrees as follows:

A. Permitted Uses and Disclosures of PHI.

(1) General Use and Disclosure. Except as otherwise limited in this Agreement, Physicians Insurance RRG may use or disclose PHI on behalf of Covered Entity as necessary to provide services as set forth in the Services Agreement, if such use or disclosure of PHI would not violate HIPAA if done by Covered Entity. Physicians Insurance RRG shall maintain the privacy and security of all PHI in accordance with the requirements of HIPAA and any and all applicable state and federal laws, rules, regulations, and orders in effect. Physicians Insurance RRG will not use or disclose the information other than as permitted by the terms of this Agreement or as required by HIPAA and/or other applicable law.

(2) Business Activities of Physicians Insurance RRG. Unless otherwise limited herein, Physicians Insurance RRG may use and/or disclose PHI:

2.1 As necessary for the proper management and administration of Physicians Insurance RRG or to carry out the legal responsibilities of Physicians Insurance RRG provided that;

(i) The disclosure is required by law; or

(ii) Physicians Insurance RRG has obtained reasonable assurances from the person to whom the PHI is disclosed that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person and that Physicians Insurance RRG will be notified of any instances of which the person is aware in which the confidentiality of the information is breached.

2.2 To provide Data Aggregation services as permitted by HIPAA;

2.3 To de-identify PHI pursuant to HIPAA standards;

2.4 As required by law.

B. Responsibilities of Physicians Insurance RRG.

With regard to its use and/or disclosure of PHI, Physicians Insurance RRG hereby agrees to do the following:

(1) Use of PHI. Not use or further disclose PHI other than as permitted or required by the Services Agreement, this Agreement, or as required by law.

(2) Minimum Necessary. Make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request;

(3) Physicians Insurance RRG's Subcontractor. Enter into a Business Associate Agreement with any subcontractor that creates, receives, maintains, or transmits PHI on behalf of Physicians Insurance RRG provided that the subcontractor agrees to comply with HIPAA and agrees to conditions and restrictions that are substantially similar to those that apply through this Agreement to Physicians Insurance RRG with respect to such PHI consistent with 45 CFR § 164.502(e).

(4) Reporting of Breach. Report to the Covered Entity any use or disclosure of protected health information not provided for by this Agreement of which Physicians Insurance RRG becomes aware, including breaches of unsecured PHI as required by 45 CFR § 164.410 and/or other applicable law.

(5) Internal Practices, Books and Records. Make its internal practices, books, and records related to the use and disclosure of PHI received from, or created or maintained by Physicians Insurance RRG on behalf of the Covered Entity, available to the

Secretary of the Department of Health and Human Services (the "Secretary") or a state regulatory body for the purposes of determining compliance with HIPAA and/or other applicable law.

(6) Security. Use appropriate safeguards to prevent use or disclosure of PHI not permitted by this Agreement, HIPAA or state law and to protect the confidentiality, integrity, and availability of electronic PHI that Physicians Insurance RRG creates, receives, maintains, or transmits in accordance with the requirements and standards and implementation specifications of the Security Rule published at 45 CFR Parts 160 and 164.

(7) Security Incidents. Report to the Covered Entity any Security Incident of which it becomes aware that results in the unauthorized access, use, disclosure, modification or destruction of electronic PHI or interference with Physicians Insurance RRG's system operations in its information system. To the extent probes and reconnaissance scans constitute Security Incidents, no additional notice shall be requested from Physicians Insurance RRG so long as the probes or reconnaissance scans do not result in unauthorized access, use or disclosure of PHI.

(8) Access to Designated Record Set. To the extent that Physicians Insurance RRG maintains PHI in a "Designated Record Set," as such term is defined in 45 CFR § 164.501, on behalf of Covered Entity, Physicians Insurance RRG shall make the PHI in the Designated Record Set available to the Covered Entity so that the Covered Entity may meet its access obligations under 45 CFR § 164.524. If the Covered Entity requests an electronic copy of PHI that is maintained by Physicians Insurance RRG electronically in a Designated Record Set, Physicians Insurance RRG will provide an electronic copy in the form and format specified by the Covered Entity unless it is not readily producible in such format, in which case it shall be produced in standard hard copy format. Physicians Insurance RRG may charge a reasonable cost-based fee for copying the Designated Record Set.

(9) Amendment of PHI in Designated Record Set. Amend PHI in a Designated Record Set that Covered Entity directs or make available to Covered Entity for amendment of PHI maintained by Physicians Insurance RRG in a Designated Record Set within ten (10) business days of a written request by Covered Entity in order to permit Covered Entity to comply with an Individual's request for an amendment in accordance with 45 CFR § 164.526.

(10) Document Disclosures. Document such disclosures 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 with 45 CFR § 164.528. Within ten (10) business days of a written request by Covered Entity, Physicians Insurance RRG agrees to provide to Covered Entity information collected in accordance with this Section in order for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. If Physicians Insurance RRG receives a request from an individual or an individual's designee for PHI, Physicians Insurance RRG shall forward any such request to Covered Entity within ten (10) business days and will coordinate any responsive communication to the request as directed by Covered Entity.

C. Responsibilities of Covered Entity

(1) Notification of Restrictions. Covered Entity shall promptly notify Physicians Insurance RRG in writing of any restrictions on the use or disclosure of an individual's PHI that 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 Physicians Insurance RRG's use or disclosure of PHI.

(2) Notification of Privacy Practices. Covered Entity shall promptly notify Physicians Insurance RRG of any limitations in the form or notice of privacy practices that Covered Entity provides to individuals pursuant to 45 CFR § 164.520, to the extent that such limitation may affect Physicians Insurance RRG's use or disclosure of PHI.

D. General Requirements

(1) Term. This Agreement shall be effective when the coverage commences pursuant to the terms of the applicable insurance policy issued to Covered Entity or the effective date of the applicable Services Agreement and shall continue in effect until all PHI provided by Covered Entity to Physicians Insurance RRG, or created or received by Physicians Insurance RRG on behalf of Covered Entity, is destroyed or returned to Covered Entity in accordance with this Section D(3), or unless terminated as provided herein or by the mutual agreement of the Parties.

(2) Termination for Cause. If either party determines that the other party has breached a material term of this Agreement, such party shall, at its option and in its sole discretion, do one of the following:

2.1 Subject to Physicians Insurance RRG's regulatory requirements, immediately terminate this Agreement;

2.2 Provide the other party with thirty (30) days written notice of the existence of an alleged material breach and afford the other party an opportunity to cure said alleged breach to the satisfaction of such party within such thirty (30) day period. The other party's failure to cure shall be grounds for immediate termination of this Agreement subject to Physicians Insurance RRG's regulatory requirements; or

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

(3) Effect of Termination. Upon termination of this Agreement, Physicians Insurance RRG shall return all PHI received from, or created or received by Physicians Insurance RRG on behalf of the Covered Entity that is then maintained in any form by Physicians Insurance RRG or its subcontractors, or if expressly requested to do so by the Covered Entity, Physicians Insurance RRG shall destroy such PHI and provide the Covered Entity documentation evidencing such destruction. Physicians Insurance RRG shall retain no copies of such PHI except as follows. If Physicians Insurance RRG determines that return or destruction of PHI is not feasible, Physicians Insurance RRG shall provide notice to the Covered Entity of the conditions that make return or destruction infeasible, and shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Physicians Insurance RRG maintains such PHI.

(4) Prohibition on Sale of PHI. Except as expressly permitted by HIPAA and state law, Physicians Insurance RRG shall refrain from receiving any remuneration in exchange for an individual's PHI unless that exchange is pursuant to a valid authorization that meets the requirements of 45 CFR § 164.508.

(5) No Third Party Beneficiaries. Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Physicians Insurance RRG and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

(6) Definitions. Terms used in this Agreement shall have the same meaning as those terms in 45 CFR Parts 160 and 164.

William Cotter
President
Physicians Insurance Risk Retention Group, Inc.