

This Agreement replaces all prior Business Associate Agreements with Physicians Insurance A Mutual Company (“Physicians Insurance”).

WHEREAS Physicians Insurance and its subsidiaries (together “the Company”) are “Business Associates” of certain “Covered Entities” 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 the Company 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 the Company’s insureds and other customers who disclose PHI to the Company 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. The Company agrees as follows:

A. Permitted Uses and Disclosures of PHI.

- (1) General Use and Disclosure. Except as otherwise limited in this Agreement, the Company 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. The Company 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. The Company 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 the Company. Unless otherwise limited herein, the Company may use and/or disclose PHI:
 - 2.1 As necessary for the proper management and administration of the Company or to carry out the legal responsibilities of the Company provided that:
 - (i) The disclosure is required by law; or
 - (ii) The Company 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 the Company 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 the Company.

With regard to its use and/or disclosure of PHI, the Company 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) Company’s Subcontractor. Enter into a Business Associate Agreement with any subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Company providing that the subcontractor agrees to comply with HIPAA and agrees to conditions and restrictions that are substantially similar to those apply through this Agreement to the Company 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 the Company 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 the Company 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 the Company creates, receives, maintains, or transmits in accordance with the requirements and standards and implementation specifications of the Security Rule published at 45 CFR Parts 160-164.
- (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 the Company’s

system operations in its information system. To the extent probes and reconnaissance scans constitute Security Incidents, no additional notice shall be requested from the Company 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 the Company maintains PHI in a "Designated Record Set," as such term is defined in 45 CFR § 164.501, on behalf of Covered Entity, the Company 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 the Company electronically in a Designated Record Set, the Company 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. The Company 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 PHI maintained by the Company 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, the Company 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 the Company receives a request from an individual or an individual's designee for PHI, the Company 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 the Company 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 the Company's use or disclosure of PHI.
- (2) Notification of Privacy Practices. Covered Entity shall promptly notify the Company 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 the Company'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 the Company, or created or received by the Company 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, either
 - 2.1 Subject to the Company'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 the Company'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, the Company shall return all PHI received from, or created or received by the Company on behalf of the Covered Entity that is then maintained in any form by the Company or its subcontractors, or if expressly requested to do so by the Covered Entity, the Company shall destroy such PHI and provide the Covered Entity documentation evidencing such destruction. The Company shall retain no copies of such PHI except as follows. If the Company determines that return or destruction of PHI is not feasible, the Company 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 the Company maintains such PHI.
- (4) Prohibition on Sale of PHI. Except as expressly permitted by HIPAA and state law, the Company 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, the Company 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 Part 160, Part 162, and Part 164.



William Cotter
President and CEO
Physicians Insurance A Mutual Company