



**PACIFIC GENERAL  
FINANCIAL**

**BUSINESS ASSOCIATE AGREEMENT  
(The HITECH Act VERSION)**

This Business Associate Agreement (the “**Agreement**”), dated February 17th, 2010, is entered into by and between (GROUP NAME) (“**Covered Entity**”) and **Pacific General Underwriters of Georgia, Inc.** (each a “**Party**” and collectively the “**Parties**”).<sup>1</sup>

**Recitals**

WHEREAS, Covered Entity has engaged Business Associate to perform services on its behalf;

WHEREAS, Covered Entity possesses Individually Identifiable Health Information that is protected under HIPAA, the HIPAA Privacy Regulations, the HIPAA Security Regulations and the HITECH Standards and is permitted to use or disclose such information only in accordance with such laws and regulations;

WHEREAS, Business Associate may receive such information from Covered Entity or create and receive such information on behalf of Covered Entity;

WHEREAS, Covered Entity wishes to ensure that Business Associate will appropriately safeguard Individually Identifiable Health Information;

NOW THEREFORE, for good and valuable consideration, the sufficiency of which we hereby acknowledge, the Parties agree as follows:

**Article 1  
Definitions**

Terms used but not otherwise defined in this Agreement shall have the same meaning as the meaning ascribed to those terms in the Health Information Portability and Accountability Act of 1996, codified as 42 U.S.C. §1320d (“**HIPAA**”), the Health Information Technology Act of 2009, as codified at 42 U.S.C.A. prec. § 17901 (the “**HITECH**” Act), and any current and future regulations promulgated under HIPAA or HITECH.

1.1 “**Breach**” shall mean the acquisition, access, use or disclosure of Protected Health Information in a manner not permitted under 45 C.F.R. Part 164, Subpart E (the “**HIPAA Privacy Regulations**”) which compromises the security or privacy of the Protected Health Information. “Breach” shall not include:

---

<sup>1</sup> If you are uncertain whether a Business Associate relationship exists, add the following provision: “Execution of this Agreement is not an admission that a business association relationship exists between the Parties as defined in HIPAA and corresponding regulations.”

(a) Any unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of Covered Entity or Business Associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Regulations; or

(b) Any inadvertent disclosure by a person who is authorized to access Protected Health Information at Covered Entity or Business Associate to another person authorized to access Protected Health Information at Covered Entity or Business Associate, respectively, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Regulations; or

(c) A disclosure of Protected Health Information where Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

1.2 **“Designated Record Set”** means a group of records maintained by or for a Covered Entity that is (a) the medical and billing records about Individuals maintained by or for a covered healthcare provider; (b) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan, or (c) information used in whole or in part by or for the Covered Entity to make decisions about Individuals.

1.3 **“Electronic Protected Health Information”** or **“Electronic PHI”** means Protected Health Information that is transmitted by or maintained in electronic media as defined by the HIPAA Security Regulations.

1.4 **“Individual”** shall have the same meaning as the term “individual” in 45 C.F.R. §164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502(g).

1.5 **“HIPAA Privacy Regulations”** shall mean the Standards for Security of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.

1.6 **“HIPAA Security Regulations”** shall mean the Standards for Security of Individually Identifiable Health Information at 45 C.F.R. part 160 and subparts A and C of part 164.

1.7 **“HITECH Standards”** means the privacy, security and security Breach notification provisions applicable to a Business Associate under Subtitle D of the HITECH Act and any regulations promulgated thereafter.

1.8 **“Individually Identifiable Information”** means information that is a subset of health information, including demographic information collected from an individual, and:

(a) is created or received by a health care provider, health plan, employer or health care clearinghouse; and

(b) relates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and:

- (i) that identifies the individual; or
- (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

1.9 **“Protected Health Information”** or **“PHI”** shall have the same meaning as the term “protected health information” in 45 C.F.R. §160.103 (as amended by the HITECH Act), limited to the information created or received by Business Associate from or on behalf of Covered Entity including, but not limited to Electronic PHI.

1.10 **“Secretary”** shall mean the Secretary of the Department of Health and Human Services or his/her designee.

1.11 **“Unsecured Protected Health Information”** shall mean Electronic PHI that is not secured through the use of technology or methodology specified by the Secretary in regulations or as otherwise defined in section 13402(h) of the HITECH Act.

## **Article 2**

### **Obligations of Business Associate**

2.1 **Limited Use or Disclosure of PHI.** Business Associate agrees to not use or further disclose PHI other than as permitted or required by the Agreement or as required by law. Business Associate may (1) use and disclose PHI to perform the services agreed to by the Parties; (2) use or disclose PHI for the proper management and administration of Business Associate or in accordance with its legal responsibilities; (3) use PHI to provide data aggregation services relating to health care operations of Covered Entity; (4) use or disclose PHI to report violations of the law to law enforcement; or (5) use PHI to create de-identified information consistent with the standards set forth at 45 C.F.R. §164.514. Business Associate will not sell PHI or use or disclose PHI for marketing or fund raising purposes as set forth in the HITECH Act.

2.2 **Subcontractors.** Business Associate agrees to require any subcontractor to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, to agree to the same restrictions and conditions that apply throughout this Agreement to Business Associate with respect to such information.

2.3 **Safeguards.** Business Associate agrees to use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

2.4 **Mitigation.** Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Association in violation of this Agreement.

## 2.5 Notice of Use or Disclosure, Security Incident or Breach.

(a) Business Associate agrees to notify the designed Privacy Officer of the Covered Entity of any use or disclosure of PHI by Business Associate not permitted by this Agreement, any Security Incident (as defined in 45 C.F.R. §164.304) involving Electronic PHI, and any Breach of Unsecured Protected Health Information without unreasonable delay, but in no case more than thirty (30) days<sup>2</sup> following discovery of breach. Business Associate shall provide the following information in such notice to Covered Entity:

- (i) the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach;
- (ii) a description of the nature of the Breach including the types of unsecured PHI that were involved, the date of the Breach and the date of discovery;
- (iii) a description of the type of Unsecured PHI acquired, accessed, used or disclosed in the Breach (e.g., full name, social security number, date of birth, etc.);
- (iv) the identity of the person who made and who received (if known) the unauthorized acquisition, access, use or disclosure;
- (v) a description of what the Business Associate is doing to mitigate the damages and protect against future breaches; and
- (vi) any other details necessary for Covered Entity to assess risk of harm to Individual(s), including identification of each Individual whose unsecured PHI has been Breached and steps such Individuals should take to protect themselves.

(b) Covered Entity will be responsible for providing notification to Individuals whose unsecured PHI has been disclosed, as well as the Secretary and the media, as required by the HITECH Act.

(c) Business Associate agrees to establish procedures to investigate the Breach, mitigate losses, and protect against any future Breaches, and to provide a description of these procedures and the specific findings of the investigation to Covered Entity in the time and manner reasonably requested by Covered Entity.

(d) The Parties agree that this section satisfies any notice requirements of Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional

---

<sup>2</sup> The HITECH Act requires the covered entity to provide notification to individuals and the media in certain cases within 60 days of when the breach is discovered. According to the Interim Final Rule published by the Office of Civil Rights (OCR), Department of Health and Human Services (HHS) on August 24, 2009 the Secretary of HHS will "attribute knowledge of a breach by a workforce member or other agent (other than the person committing the breach) to the covered entity itself." This means when the business associate discovered the breach. Thus, the business associate must provide timely notice to the covered entity to enable the covered entity to meet its deadline. Keep this in mind when negotiating timeframes for reporting breaches.

notice to Covered Entity shall be required. For purposes of this Agreement, “**Unsuccessful Security Incidents**” include activity such as pings and other broadcast attacks on Business Associate’s firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of Electronic PHI.

2.6 **Access.** Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner reasonably requested by Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual. Business Associate may charge Covered Entity or Individual for the actual labor cost involved in providing such access.

2.7 **Amendments.** Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees, upon request of Covered Entity or an Individual.

2.8 **Disclosure of Practices, Books and Records.** Business Associate agrees to make internal practices, books and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, available to Covered Entity or the Secretary in a time and manner designated by the Covered Entity or Secretary, for the purposes of the Secretary in determining the Parties compliance with HIPAA, the HITECH Act and corresponding regulations.

2.9 **Accounting.** Business Associate agrees to provide to Covered Entity an accounting of PHI disclosures made by Business Associate, including disclosures made for treatment, payment and health care operations. The accounting shall be made within a reasonable amount of time upon receipt of a request from Covered Entity.

2.10 **Security of Electronic Protected Health Information.** Business Associate agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of Covered Entity; (2) ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; and (3) report to the Covered Entity any security incidents of which it becomes aware.

2.11 **Minimum Necessary.** To limit its uses and disclosures of, and requests for, PHI (a) when practical, to the information making up a Limited Data Set; and (b) in all other cases subject to the requirements of 45 C.F.R. §164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

2.12 **Indemnification.** Each Party shall indemnify and hold harmless the other Party and its affiliates, directors, officers, employees, partners, contractors or agents, from and against any and all claims, actions, causes of action, demands, or liabilities of whatsoever kind and nature, including judgments, interest, reasonable attorneys’ fees, and all other costs, fees, expenses, and

charges (collectively, “**Claims**”) to the extent that such Claims arise out of or were caused by the negligence, gross negligence, or willful misconduct of the indemnifying Party or from any material breach of the Agreement by the indemnifying Party.

2.13 **Permitted Uses and Disclosures.** Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity provided that such use or disclosure would not violate HIPAA or the HITECH Act if done by the Covered Entity.

### **Article 3** **Obligations of Covered Entity**

3.1 **Notice of Privacy Practices of Covered Entity.** Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 C.F.R. §164.520, as well as any changes to such notice.

3.2 **Restrictions in Use of PHI.** Covered Entity shall notify Business Associate of any changes restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed, to the extent that such restriction may affect Business Associate’s use or disclosure of PHI.

3.3 **Changes in the Use of PHI.** Covered Entity agrees to notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent such changes or revocation affects Business Associate’s use or disclosure of PHI.

3.4 **Appropriate Requests.** Except as otherwise provided in this Agreement, Covered Entity will not ask Business Associate to use or disclose PHI in any manner that would violate the HIPAA Privacy Regulations or the HITECH Act of done by Covered Entity.

### **Article 4** **Term and Termination**

4.1 **Term.** The Term of this Agreement shall be effective as of the date listed above and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section.

4.2 **Termination for Cause.** Upon either Party’s determination that the other Party has committed a violation or material breach of this Agreement, the non-breaching Party may take one of the following steps:

(a) Provide an opportunity for the breaching Party to cure the breach or end the violation, and if the breaching Party does not cure the breach or end the violation within a reasonable time, terminate this Agreement;

(b) Immediately terminate this Agreement if the other Party has committed a material breach of this Agreement and cure of the material breach is not possible; or

(c) If neither cure nor termination is feasible, elect to continue this Agreement and report the violation or material breach to the Secretary in accordance with the requirements set forth in the HITECH Act.

#### **4.3 Effect of Termination.**

(a) Upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors of Business Associate.

(b) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

### **Article 5** **Miscellaneous**

5.1 **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for covered Entity to comply with the requirements of HIPAA or the HITECH Act and any applicable regulations in regard to such laws.

5.2 **Survival.** The respective rights and obligations of Business Associate shall survive the termination of this Agreement.

5.3 **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA or the HITECH Act or any applicable regulations in regard to such laws.


5.4 **Prior Agreement.** This Agreement shall replace and supersede any prior Business Associate Agreement between the Parties.



5.5 **Ambiguity.** Any ambiguity of this Agreement shall be resolved to permit the Parties to comply with the HITECH Act, HIPAA, and the Privacy and Security Rules and other implementing regulations and guidance.

IN WITNESS WHEREOF, the Parties hereby execute this Agreement to be effective as of the date written above. Execution of this Agreement is not an admission that a business association relationship exists between the Parties as defined in HIPAA and corresponding regulations.

Pacific General Underwriters of Georgia, Inc.

By: 

Signature

Scott A. Burrell, President

**GROUP NAME**

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

Signature

\_\_\_\_\_  
(Print Name  
& Title)