

New Business Associate Agreement and Training

The United States Department of Health and Human Services (HHS) recently published new rules about breaches of “unsecured protected health information.” These rules apply to BlueCross BlueShield of South Carolina and our agents.

A breach is the acquisition, access, use or disclosure of protected health information (PHI) that is not allowed by the Health Information Portability and Accountability Act (HIPAA). A breach could compromise the security or privacy of PHI. It does not matter if the information is printed, electronic or verbal. Here are a few examples:

- Sending a completed application to the wrong client for signature
- Sending an e-mail containing PHI to the wrong person
- Sharing a person’s PHI with any other person who is not authorized to see the information

In order to comply with the new regulations, we have revised our Business Associate Agreement (BAA). ALL agents appointed with BlueCross and/or BlueChoice HealthPlan must read, sign and return the new BAA no later than February 17, 2010. Please fax the signed agreement to 803-870-8068. You may also e-mail the signed agreement to grpandindv@bcssc.com. You will find a copy of the new agreement attached to this bulletin.

Additionally, we are requiring agents to complete a brief training course on the Learning Management System (LMS) to show they have read and understand the new regulations. The course, HITECH for Agents, is now available on LMS. You can find the course in the Required Courses section of LMS.

Please contact your marketing rep with additional questions.

BlueChoice HealthPlan is an independent licensee of the Blue Cross and Blue Shield Association



South Carolina

BlueCross BlueShield of South Carolina
is an independent licensee of the
Blue Cross and Blue Shield Association

AGREEMENT WITH BUSINESS ASSOCIATE

This Agreement (“BAA”) is effective upon execution, and is made by and between the undersigned Agent/Agency (“Business Associate”) and Blue Cross and Blue Shield of South Carolina (“BCBSSC”), BlueChoice HealthPlan of South Carolina, Inc. and Companion Life Insurance Company (BCBSSC, its subsidiaries and affiliates are collectively referred to as “Company”).

Company and Business Associate mutually agree to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing regulations (45 C.F.R. Parts 160-64) and the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”), that are applicable to business associates, along with any guidance and/or regulations issued by DHHS. Company and Business Associate agree to incorporate into this Agreement any regulations issued with respect to the HITECH Act that relate to the obligations of business associates. Business Associate recognizes and agrees that it is obligated by law to meet the applicable provisions of the HITECH Act.

A. Privacy & Security of Protected Health Information and Electronic Protected Health Information.

1. **Permitted Uses and Disclosures.** Business Associate is permitted or required to use or disclose Protected Health Information (“PHI”) and electronic PHI it creates or receives for or from Company or to request PHI and electronic PHI on Company’s behalf only as follows:
 - a) **Functions and Activities on Company’s Behalf.** To perform functions, activities, services, and operations on behalf of Company, consistent with HIPAA, the HITECH Act, and their implementing regulations as specified in the Producer Appointment Agreement.
 - b) **Business Associate’s Operations.** Business Associate may use the Minimum Necessary PHI and electronic PHI for Business Associate’s proper management and administration or to carry out Business Associate’s legal responsibilities. Business Associate may disclose the Minimum Necessary PHI and electronic PHI for Business Associate’s proper management and administration or to carry out Business Associate’s legal responsibilities only if:
 - (i) The disclosure is required by law; or
 - (ii) Business Associate obtains reasonable assurance, evidenced by written contract, from any person or organization to which Business Associate will disclose PHI or electronic PHI that the person or organization will:
 - a. Hold such PHI, electronic PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization or as Required by Law; and
 - b. Promptly notify Business Associate (who will in turn promptly notify Company) of any instance of which the person or organization becomes aware in which the confidentiality of such PHI or electronic PHI was breached.
2. **Minimum Necessary and Limited Data Set.** Business Associate’s use, disclosure or request of Protected Health Information shall utilize a Limited Data Set if practicable. Otherwise, Business Associate will, in its performance of the functions, activities, services, and operations specified in Section A.1(a) above, make reasonable efforts to use, to disclose, and to request of a Covered Entity only the minimum amount of Company’s Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request.
3. **Prohibition on Unauthorized Use or Disclosure.** Business Associate will neither use nor disclose PHI or electronic PHI except as permitted or required by this Agreement, as otherwise permitted in writing by Company, or as required by law. This Agreement does not authorize Business Associate to use or disclose PHI or electronic PHI in a manner that would violate the requirements of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R. Parts 160-64) or the HITECH Act and its implementing regulations, if done by Company, except as set forth in Section A(1)(b).

4. **Information Safeguards.** Business Associate will develop, document, implement, maintain, and use appropriate administrative, technical, and physical safeguards, in compliance with Social Security Act § 1173(d) (42 U.S.C. § 1320d-2(d)), 45 C.F.R. Part 164, Subparts C & E, and any other implementing regulations issued by the U.S. Department of Health and Human Services (including, but not limited to, CMS Core Security Requirements, if applicable), and any other applicable laws. The safeguards will be designed to preserve the integrity, availability and confidentiality of electronic PHI, and to prevent intentional or unintentional non-permitted or violating use or disclosure of, PHI. Business Associate will additionally develop any safeguards to the extent required by the HITECH Act. Business Associate will document and keep these safeguards current. Business Associate agrees to mitigate any harmful effect that is known to the Business Associate resulting from a use or disclosure of PHI or electronic PHI by the Business Associate or its subcontractors in violation of the requirements of this Agreement.
5. **Subcontractors and Agents.** Business Associate will require any of its subcontractors and agents, to which Business Associate is permitted by this Agreement or in writing by Company to disclose PHI and electronic PHI, to provide reasonable assurance, evidenced by written contract, that such subcontractor or agent will comply with the same privacy and security obligations as Business Associate with respect to such PHI and, electronic PHI.

B. Compliance with Standard Transactions. If Business Associate conducts, in whole or part, Standard Transactions for or on behalf of Company, Business Associate will comply, and will require any subcontractor or agent involved with the conduct of such Standard Transactions to comply, with each applicable requirement of 45 C.F.R. Part 162. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any Trading Partner Agreement in connection with the conduct of Standard Transactions for or on behalf of Company that:

1. Changes the definition, data condition, or use of a data element or segment in a Standard Transaction;
2. Adds any data element or segment to the maximum defined data set;
3. Uses any code or data element that is marked “not used” in the Standard Transaction’s implementation specification or is not in the Standard Transaction’s implementation specification; or
4. Changes the meaning or intent of the Standard Transaction’s implementation specification.

C. Individual Rights.

1. **Access.** Business Associate will, within five (5) business days after Company’s request, make available to Company or, at Company’s direction, to the individual (or the individual’s personal representative) for inspection and obtaining copies any PHI and electronic PHI about the individual that is in Business Associate’s custody or control, so that Company may meet its access obligations under 45 C.F.R. § 164.524 and, where applicable, the HITECH Act. Business Associate shall make such information available in an electronic format where directed by Company.
2. **Amendment.** Business Associate will, upon receipt of notice from Company, promptly amend or permit Company access to amend any portion of the PHI and electronic PHI, so that Company may meet its amendment obligations under 45 C.F.R. § 164.526.
3. **Disclosure Accounting.** So that Company may meet its disclosure accounting obligations under 45 C.F.R. § 164.528:
 - a) **Disclosure Tracking.** Business Associate will record information concerning each disclosure of PHI or electronic PHI, not excepted from disclosure tracking under Agreement Section C.3(b) below, that Business Associate makes to Company or a third party. The Disclosure Information Business Associate will record includes: (i) the disclosure date; (ii) the name and (if known) address of the person or entity to whom Business Associate made the disclosure; (iii) a brief description of the PHI or electronic PHI disclosed; and (iv) a brief statement of the purpose of the disclosure (items i-iv, collectively, the “disclosure information”). Business Associate further shall provide any additional information to the extent required by the HITECH Act and any accompanying regulations. For repetitive disclosures Business Associate makes to the same person or entity for a single purpose, Business Associate may provide (x) the disclosure information for the first of these repetitive disclosures; (y) the frequency, periodicity or number of these repetitive disclosures; and (z) the date of the last of these repetitive disclosures.

Business Associate will make this disclosure information available to Company within ten (10) business days after Company’s request.

- b) **Exceptions from Disclosure Tracking.** Business Associate need not record disclosure information or otherwise account for disclosures of PHI or electronic PHI that this Agreement or Company in writing permits or requires (i) for purposes of Treating the individual who is the subject of the PHI or electronic PHI disclosed, payment for that Treatment, or for the Health Care Operations of Company or Business Associate (except where such recording or accounting is required by the HITECH Act, and as of the effective dates for this provision of the HITECH Act); (ii) to the individual who is the subject of the PHI or electronic PHI disclosed or to that individual's personal representative; (iii) pursuant to a valid authorization by the person who is the subject of the PHI or electronic PHI disclosed; (iv) to persons involved in that individual's health care or Payment related to that individual's health care; (v) for notification for disaster relief purposes; (vi) for national security or intelligence purposes; (vii) as part of a Limited Data Set; or (viii) to law enforcement officials or correctional institutions regarding inmates or other persons in lawful custody.
 - c) **Disclosure Tracking Time Periods.** Unless otherwise provided under the HITECH Act, Business Associate must have available for Company the disclosure information required by Agreement Section C.3(a) for the six (6) years preceding Company's request for the disclosure information. In addition, where Business Associate is contacted directly by an individual based on information provided to the individual by Company, and where so required by the HITECH Act and/or any accompanying regulations, Business Associate shall make such Disclosure Information available directly to the individual.
4. **Restriction Requests; Confidential Communications.** Business Associate shall immediately notify Company's Privacy Officer of any individual request made pursuant to 45 C.F.R. § 164.522 that Company or Business Associate restrict the disclosure of protected health information of the individual. Business Associate will comply with any requests for restriction requests and confidential communications of which it is aware and to which Company agrees pursuant to 45 C.F.R. § 164.522 (a) and (b).
5. **Inspection of Books and Records.** Business Associate will make its internal practices, books, and records, relating to its use and disclosure of PHI or electronic PHI, available to Company and to the U.S. Department of Health and Human Services to determine compliance with 45 C.F.R. Parts 160-64 or this Agreement.

D. Breach of Privacy & Security Obligations.

1. **Breach.** Business Associate will report to Company any use or disclosure of PHI or electronic PHI not permitted by this Agreement or by Company in writing. Business Associate will make the report to Company's Privacy Officer within three (3) business days after Business Associate knew or by the exercise of reasonable diligence should have known of such non-permitted use or disclosure. In addition, Business Associate will report, following discovery and without unreasonable delay, but in no event later than three (3) business days following discovery, any "Breach" of "Unsecured Protected Health Information" as these terms are defined by the HITECH Act and any implementing regulations, even if Business Associate deems the unauthorized acquisition, access or use to be in good faith, unintentional or inadvertent and even if Business Associate deems the risk of harm posed to the individuals involved to be insignificant. Business Associate shall cooperate with Company in investigating the Breach and in meeting the Company's obligations under the HITECH Act and any other security breach notification laws.

Any such report shall include the identification (if known) of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate's report will, at a minimum:

- a) Identify the nature of the non-permitted access, use or disclosure, including the date of the Breach and the date of discovery of the Breach;
- b) Identify the PHI or electronic PHI accessed, used or disclosed as part of the Breach (e.g. full name, social security number, date of birth, etc.);
- c) Identify who made the non-permitted or violating access, use or disclosure and who received the non-permitted disclosure;
- d) Identify what corrective action Business Associate took or will take to prevent further non-permitted access, uses or disclosures;
- e) Identify what Business Associate did or will do to mitigate any deleterious effect of the non-permitted access, use or disclosure; and
- f) Provide such other information, including a written report, as Company may reasonably request.

2. **Security Incident.** Business Associate will additionally report to Company as requested by the Company any attempted or successful (a) unauthorized access, use, disclosure, modification, or destruction of Company's electronic PHI of which Business Associate becomes aware, or (b) interference with system operations in Business Associate's Information System containing Company's electronic PHI ("Security Incident") of which Business Associate becomes aware. If the Security Incident resulted in an unauthorized access, use, or disclosure, then a written report shall be provided according to the timeline and content requirements in Section D.1 above.
3. **Mitigation.** Business Associate agrees to mitigate, to the extent practicable, any harmful effect resulting from any Breach or attempted or successful Security Incident. In addition, Business Associate shall cooperate with and implement any reasonable mitigation requests by Company relating to any Breach or attempted or successful Security Incident. Any mitigation performed pursuant to this Section shall be done at Business Associate's expense.

E. General Provisions.

1. Termination of Agreement.

a) **Right to Terminate for Breach.**

- (i) Company may terminate Agreement if it determines, in its sole discretion, that Business Associate has breached any provision of this Agreement. Company may exercise this right to terminate Agreement by providing Business Associate written notice of termination, stating the breach of the Agreement that provides the basis for the termination. Any such termination will be effective immediately or at such other date specified in Company's notice of termination. If for any reason Company determines that Business Associate has breached the terms of this Agreement and such breach has not been cured, but Company determines that termination of the Agreement is not feasible, Company may report such breach to the U.S. Department of Health and Human Services.
- (ii) Business Associate may terminate Agreement if it determines, after reasonable consulting with Company, that Company has breached any material provision of this Agreement and upon written notice to Company of the breach, Company fails to cure the breach within thirty (30) days after receipt of the notice. Business Associate may exercise this right to terminate Agreement by providing Company written notice of termination, stating the failure to cure the breach of this Agreement that provides the basis for the termination. Any such termination will be effective upon such reasonable date as the parties mutually agree. If Business Associate reasonably determined that Company has breached a material provision of this Agreement and such breach has not been cured, but Business Associate and Company mutually determine that termination of the Agreement is not feasible, Business Associate may report such breach to the U.S. Department of Health and Human Services.

b) **Obligations upon Termination.**

- (i) **Return or Destruction.** Upon termination, cancellation, expiration or other conclusion of Agreement, Business Associate will, if feasible, return to Company or destroy all PHI and electronic PHI in whatever form or medium (including any electronic medium) and all copies of any data or compilations derived from and allowing identification of any individual who is a subject of PHI and electronic PHI. Company will determine, in its sole discretion, whether Business Associate will destroy or return such PHI and electronic PHI. Business Associate will complete such return or destruction as promptly as possible, but not later than ten (10) business days after the effective date of the termination, cancellation, expiration or other conclusion of Agreement. All costs related to the Business Associate's return or destruction of PHI and electronic PHI will be paid by the Business Associate. Business Associate will identify any PHI and electronic PHI that cannot feasibly be returned to Company or destroyed. Business Associate will limit its further use or disclosure of that PHI and electronic PHI to those purposes that make return or destruction of that PHI and electronic PHI infeasible. Within ten (10) business days after the effective date of the termination, cancellation, expiration or other conclusion of Agreement, Business Associate will (a) certify on oath in writing to Company that such return or destruction has been completed, (b) deliver to Company the identification of any PHI and electronic PHI for which return or destruction is infeasible, and (c) certify that it will only use or disclose such PHI and electronic PHI for those purposes that make return or destruction infeasible.
- (ii) **Continuing Privacy Obligation.** Business Associate's obligation to protect the privacy of the PHI and electronic PHI it created or received for or from Company will be continuous and survive termination, cancellation, expiration or other conclusion of Agreement.

- c) **Other Obligations and Rights.** Business Associate's other obligations and rights and Company's obligations and rights upon termination, cancellation, expiration or other conclusion of Agreement will be those set out in the Agreement.
2. **Indemnity.** Business Associate will indemnify and hold harmless Company and any Company affiliate, officer, director, employee or agent from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any non-permitted or violating use or disclosure of PHI and electronic PHI or other breach of this Agreement by Business Associate or any subcontractor, agent, person or entity under Business Associate's control.
- a) **Right to Tender or Undertake Defense.** If Company is named a party in any judicial, administrative or other proceeding arising out of or in connection with any non-permitted or violating use or disclosure of PHI and electronic PHI or other breach of this Agreement by Business Associate or any subcontractor, agent, person or entity under Business Associate's control, Company will have the option at any time to either: (i) tender its defense to Business Associate, in which case Business Associate will provide qualified attorneys, consultants, and other appropriate professionals to represent Company's interests at Business Associate's expense, or (ii) undertake its own defense, choosing the attorneys, consultants, and other appropriate professionals to represent its interests, in which case Business Associate will be responsible for and pay the reasonable fees and expenses of such attorneys, consultants, and other professionals.
- b) **Right to Control Resolution.** Company will have the sole right and discretion to settle, compromise or otherwise resolve any and all claims, causes of actions, liabilities or damages against it, notwithstanding that Company may have tendered its defense to Business Associate. Any such resolution will not relieve Business Associate of its obligation to indemnify Company under this Agreement Section E.2.
3. **Definitions.** With respect to any information created, received, maintained, or transmitted by Business Associate from or on behalf of Company or another business associate of Company ("Company Information"), the following definitions apply:
- a) The capitalized terms "Covered Entity," "Electronic Protected Health Information ("electronic PHI" or "ePHI" shall be construed to be "Electronic Protected Health Information"), "Protected Health Information" ("PHI" shall be construed to be "Protected Health Information"), "Standard," "Trading Partner Agreement," and "Transaction" have the meanings set out in 45 C.F.R. § 160.103.
- b) The term "Standard Transactions" shall have the meaning set out in 45 C.F.R. § 162.103. The term "Minimum Necessary" shall have the meaning set out in 45 C.F.R. § 164.502.
- c) The term "Required by Law" has the meaning set out in 45 C.F.R. § 164.103.
- d) The terms "Health Care Operations," "Payment," "Research," and "Treatment" have the meanings set out in 45 C.F.R. § 164.501.
- e) The term "Limited Data Set" has the meaning set out in 45 C.F.R. § 164.514(e). The term "use" means, with respect to PHI, utilization, employment, examination, analysis or application within Business Associate.
- f) The terms "disclose" and "disclosure" mean, with respect to PHI, release, transfer, providing access to or divulging to a person or entity not within Business Associate.
- g) Any other capitalized terms not identified here shall have the meaning as set forth in 45 Code of Federal Regulations ("C.F.R.") Parts 160-64 for the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), or in the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act").
4. **Owner of Protected Health Information.** Company is the exclusive owner of PHI and electronic PHI generated or used under the terms of the Agreement or this Agreement.
5. **Amendment to Agreement.** Upon the effective date of any final regulation or amendment to final regulations promulgated by the U.S. Department of Health and Human Services with respect to PHI, electronic PHI or Standard Transactions, this Agreement will automatically amend such that the obligations they impose on Business Associate remain in compliance with these regulations.

