

Business Associate Agreement

**Prepared by the
NCHICA Contracts Work Group**

**Approved for Public Distribution
April 2, 2003**

BUSINESS ASSOCIATE AGREEMENT¹

This Agreement is made effective the ____ of ____, 200_, by and between _____, hereinafter referred to as "Covered Entity", and _____, hereinafter referred to as "Business Associate", (individually, a "Party" and collectively, the "Parties").

WITNESSETH:

WHEREAS, Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, known as "the Administrative Simplification provisions," direct the Department of Health and Human Services to develop standards to protect the security, confidentiality and integrity of health information; and

WHEREAS, pursuant to the Administrative Simplification provisions, the Secretary of Health and Human Services has issued regulations modifying 45 CFR Parts 160 and 164 (the "HIPAA Security and Privacy Rule"); and

WHEREAS, the Parties wish to enter into or have entered into an arrangement whereby Business Associate will provide certain services to Covered Entity, and, pursuant to such arrangement, Business Associate may be considered a "business associate" of Covered Entity as defined in the HIPAA Security and Privacy Rule (the agreement evidencing such arrangement is entitled _____, dated _____, and is hereby referred to as the "Arrangement Agreement"); and

WHEREAS, Business Associate may have access to Protected Health Information (as defined below) in fulfilling its responsibilities under such arrangement;

THEREFORE, in consideration² of the Parties' continuing obligations under the Arrangement Agreement, compliance with the HIPAA Security and Privacy Rule, and for Ten and 00/100s Dollars (\$10.00) and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the provisions of this Agreement in order to address the requirements of the HIPAA Security and Privacy Rule and to protect the interests of both Parties.

I. DEFINITIONS

¹This agreement is intended to meet the requirements of both the Security Regulations and Privacy Regulations of the Health Insurance Portability and Accountability Act ("HIPAA"). Given the different compliance dates of these regulations, many covered entities and business associates have entered into business associate agreements addressing only the Privacy Regulations. Covered Entities should remain mindful of the distinction between electronic protected health information and protected health information, and determine those business associates who may send or receive electronic protected health information. Covered entities that may send or receive electronic health information to or from a particular business associate should review their overall security compliance programs and determine the most appropriate time to amend their business associate agreements prior to the compliance date of the Security Regulations. Much of the language in this document has been taken directly from the regulations, and may be clarified as the regulatory language is clarified. Any deletions, additions or revisions to this Agreement may create inconsistencies within this Agreement or with other agreements, inaccuracies or otherwise render this Agreement invalid, unenforceable or non-compliant.

² The use of "Ten and 00/100s Dollars (\$10.00 and other good and valuable consideration" is fairly standard contract consideration language. The user should make a determination about whether the continuation of the relationship with the vendor is sufficient consideration and, if so, the user may consider removing the \$10.00.

Copyright (c) 2003 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/> and which is available from NCHICA upon request.

Except as otherwise defined herein, any and all capitalized terms in this Section shall have the definitions set forth in the HIPAA Security and Privacy Rule. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Security and Privacy Rule, as amended, the HIPAA Security and Privacy Rule shall control. Where provisions of this Agreement are different than those mandated in the HIPAA Security and Privacy Rule, but are nonetheless permitted by the HIPAA Security and Privacy Rule, the provisions of this Agreement shall control.

The term "Protected Health Information" means individually identifiable health information including, without limitation, all information, data, documentation, and materials, including without limitation, demographic, medical and financial information, that relates to the 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 that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. "Protected Health Information" includes without limitation "Electronic Protected Health Information" as defined below.

The term "Electronic Protected Health Information" means Protected Health Information which is transmitted by Electronic Media (as defined in the HIPAA Security and Privacy Rule) or maintained in Electronic Media.

Business Associate acknowledges and agrees that all Protected Health Information that is created or received by Covered Entity and disclosed or made available in any form, including paper record, oral communication, audio recording, and electronic display by Covered Entity or its operating units to Business Associate or is created or received by Business Associate on Covered Entity's behalf shall be subject to this Agreement.

II. CONFIDENTIALITY AND SECURITY REQUIREMENTS

- (a) Business Associate agrees:
- (i) to use or disclose any Protected Health Information solely: (1) for meeting its obligations as set forth in any agreements between the Parties evidencing their business relationship³, or (2) as required by applicable law, rule or regulation, or by accrediting or credentialing organization to whom Covered Entity is required to disclose such information or as otherwise permitted under this Agreement, the Arrangement Agreement (if consistent with this Agreement and the HIPAA Security and Privacy Rule), or the HIPAA Security and Privacy Rule, and (3) as would be permitted by the HIPAA Security and Privacy Rule if such use or disclosure were made by Covered Entity;⁴
 - (ii) at termination of this Agreement, the Arrangement Agreement (or any similar documentation of the business relationship of the Parties), or upon request of Covered Entity, whichever occurs first⁵, if feasible, Business Associate will return or destroy all Protected Health

³ Issues were raised regarding how much specificity is required regarding the types of services to be performed and the types of disclosures which would be allowed based upon those services. If the section in which services are described is not specific, a listing of specific services might be stated here in lieu of a reference to the Agreement section.

⁴ The NPRM issued on March 27, 2002 contains model Business Associate Agreement language which includes a requirement that the Covered Entity provide to the Business Associate a copy of its Notice of Privacy Practices and any amendments, as prepared, and that the Covered Entity notify the Business Associate of any restrictions in use of PHI to which the Covered Entity has agreed. Neither requirement was included in this document because these were not deemed to be required by the rule and were felt to be potentially onerous to the Covered Entity.

⁵ Although the rule doesn't require that a Business Associate return PHI at the request of a Covered Entity other than at the termination of their agreement, practical considerations suggest that this inclusion may be helpful to the Covered Entity and its compliance. It has also been suggested that in some cases, requiring a Business Associate to return all PHI prior to termination of the Copyright (c) 2003 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/> and which is available from NCHICA upon request.

Information received from or created or received by Business Associate on behalf of Covered Entity that Business Associate still maintains in any form and retain no copies of such information, or if such return or destruction is not feasible, Business Associate will extend the protections of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible; and

(iii) to ensure that its agents, including a subcontractor, to whom it provides Protected Health Information received from or created by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply to Business Associate with respect to such information, and agrees to implement reasonable and appropriate safeguards to protect any of such information which is Electronic Protected Health Information. In addition, Business Associate agrees to take reasonable steps to ensure that its employees' actions or omissions do not cause Business Associate to breach the terms of this Agreement.

(b) Notwithstanding the prohibitions set forth in this Agreement, Business Associate may use and disclose Protected Health Information as follows:

(i) if necessary, for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that as to any such disclosure, the following requirements are met:

(A) the disclosure is required by law; or

(B) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it 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 the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached;

(ii) for data aggregation services, if to be provided by Business Associate for the health care operations of Covered Entity pursuant to any agreements between the Parties evidencing their business relationship. For purposes of this Agreement, data aggregation services means the combining of Protected Health Information by Business Associate with the protected health information received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

(c) Business Associate will implement appropriate safeguards to prevent use or disclosure of Protected Health Information other than as permitted in this Agreement⁶. Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the HIPAA Security and Privacy Rule.

(d) The Secretary of Health and Human Services shall have the right to audit Business Associate's records and practices related to use and disclosure of Protected Health Information to ensure Covered Entity's compliance with the terms of the HIPAA Security and Privacy Rule.

Agreement could make it difficult for the Business Associate to continue to perform the Business Associate's obligations under the Agreement.

⁶ Issues were discussed regarding the level of responsibility which the Covered Entity has for the action/inaction of a Business Associate. With respect to safeguards, a Covered Entity may wish to set forth a list of required safeguards, however, it may be asserted that, by setting the level of safeguards, the Covered Entity may incur additional risk.

Copyright (c) 2003 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/> and which is available from NCHICA upon request.

(e) Business Associate shall report to Covered Entity any use or disclosure of Protected Health Information which is not in compliance with the terms of this Agreement of which it becomes aware. Business Associate shall report to Covered Entity any Security Incident of which it becomes aware. For purposes of this Agreement, "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. In addition, 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 Associate in violation of the requirements of this Agreement.

III. AVAILABILITY OF PHI

Business Associate agrees to make available Protected Health Information to the extent and in the manner required by Section 164.524 of the HIPAA Security and Privacy Rule⁷. Business Associate agrees to make Protected Health Information available for amendment and incorporate any amendments to Protected Health Information in accordance with the requirements of Section 164.526 of the HIPAA Security and Privacy Rule. In addition, Business Associate agrees to make Protected Health Information available for purposes of accounting of disclosures, as required by Section 164.528 of the HIPAA Security and Privacy Rule.

IV. TERMINATION

Notwithstanding anything in this Agreement to the contrary, Covered Entity shall have the right to terminate this Agreement and the Arrangement Agreement immediately if Covered Entity determines that Business Associate has violated any material term of this Agreement. If Covered Entity reasonably believes that Business Associate will violate a material term of this Agreement and, where practicable, Covered Entity gives written notice to Business Associate of such belief within a reasonable time after forming such belief, and Business Associate fails to provide adequate written assurances to Covered Entity that it will not breach the cited term of this Agreement within a reasonable period of time given the specific circumstances, but in any event, before the threatened breach is to occur, then Covered Entity shall have the right to terminate this Agreement and the Arrangement Agreement immediately.⁸

V. MISCELLANEOUS

Except as expressly stated herein or the HIPAA Security and Privacy Rule, the parties to this Agreement do not intend to create any rights in any third parties. The obligations of Business Associate under this Section shall survive the expiration, termination, or cancellation of this Agreement, the Arrangement Agreement and/or the business relationship of the parties, and shall continue to bind Business Associate, its agents, employees, contractors, successors, and assigns as set forth herein.

This Agreement may be amended or modified only in a writing signed by the Parties. No Party may assign its respective rights and obligations under this Agreement without the prior written consent of the other Party. None of the provisions of this Agreement are intended to create, nor will they be deemed to create any relationship between the Parties other than that of independent parties contracting with each other solely for

⁷ Issues were raised regarding whether a Business Associate must provide PHI directly to a patient, or whether access should always be granted only through the Covered Entity. In the event a Business Associate is not required to grant direct access, the suggestion was made that a Covered Entity might wish to require that all access be only through the Covered Entity.

⁸ Although the rule does not address injunctions and thus this provision does not refer to injunctions, a Covered Entity may wish to provide that it may seek an injunction for a breach of this Section by a Business Associate.

Copyright (c) 2003 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/> and which is available from NCHICA upon request.

the purposes of effecting the provisions of this Agreement and any other agreements between the Parties evidencing their business relationship. This Agreement will be governed by the laws of the State of North Carolina. No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

The parties agree that, in the event that any documentation of the arrangement pursuant to which Business Associate provides services to Covered Entity contains provisions relating to the use or disclosure of Protected Health Information which are more restrictive than the provisions of this Agreement, the provisions of the more restrictive documentation will control. The provisions of this Agreement are intended to establish the minimum requirements regarding Business Associate’s use and disclosure of Protected Health Information.⁹

In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event a party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Security and Privacy Rule, such party shall notify the other party in writing, For a period of up to thirty days, the parties shall address in good faith such concern and amend the terms of this Agreement, if necessary to bring it into compliance. If, after such thirty-day period, the Agreement fails to comply with the HIPAA Security and Privacy Rule, then either party has the right to terminate upon written notice to the other party.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year written above.

COVERED ENTITY:

BUSINESS ASSOCIATE:

By: _____
Title: _____

By: _____
Title: _____

⁹ A Covered Entity may wish to provide more specific references to sections of existing documentation which are intended to be more restrictive than the terms of this Agreement.
Copyright (c) 2003 by the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA), no claim to original U.S. Government Works. Any use of this document by any person is expressly subject to the user's acceptance of the terms of the User Agreement and Disclaimer that applies to this document, which may be found at <http://www.nchica.org/HIPAAResources/Samples/> and which is available from NCHICA upon request.