

# **Business Associate Agreement**

On this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_, the undersigned, (**Name of Covered Entity**) ("Covered Entity") and (**Name of Business Associate**) ("Business Associate") have entered into this "Business Associate Agreement" ("Agreement") for the purposes set forth.

## **1. Business Associate Relationship**

(a) Covered Entity and Business Associate are parties to that certain contract, denominated "(Name of underlying contract or purchase order), dated \_\_\_\_\_ ("the Contract"), and pursuant to which Business Associate is performing functions or tasks on behalf of Covered Entity.

(b) Covered Entity is bound by the regulations implementing the Health Insurance Portability and Accountability Act of 1996, P. L. 104-191 ("HIPAA"), 45 C.F.R. Parts 160 and 164 (the "Privacy Rule"). including, but not limited to, those standards comprising a subset of the Privacy Rule commonly referred to as the "Security Rule." Any reference herein to the Privacy Rule is intended to encompass those standards comprising the Security Rule, as well as the ARRA HITECH provision. It is understood that these regulations continue to be refined by the federal government, and that both the Covered Entity and the Business Associate are obligated to fulfill the requirements of any such changes. The intent and purpose of this Agreement is to comply with the requirements of the Privacy/Security Rule and related provisions, including, but not limited to, the Business Associate contract requirements at 45 C.F.R. §§ 164.502(e) and 164.504(e).

(c) In the performance of this Contract, Business Associate is performing functions on behalf of Covered Entity which meet the definition of "Business Associate Activities" in 45 C.F.R. § 160.103, and therefore Business Associate is a "Business Associate" of Covered Entity.

(d) In order for Business Associate to perform its obligations under the Contract, Covered Entity must disclose to Business Associate certain Protected Health Information (as defined in 45C.F. R. §160.103) that is subject to protection under HIPAA and the Privacy/Security Rule.

NOW, THEREFORE in consideration of the mutual promises and covenants contained herein, and in furtherance of the mutual intent of the parties to comply with the requirements of the Privacy/Security Rule, the parties agree as follows:

## **2. Definitions**

(a) **Protected Health Information.** Shall have the meaning found in 45 C.F.R. §160.103, limited to the information created, maintained, transmitted, or received by Business Associate from or on behalf of Covered Entity. "Protected Health Information may also be referred to as "PHI". PHI can take the form of oral, written, or electronic information.

(b) **Secretary.** Means the Secretary of the Department of Health and Human Services or his designee.

(c) **Individual.** Means the person who is the subject of PHI.

(d) **Administrative Safeguards.** Means administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect protected

health information and to manage the conduct of the Business Associate's workforce in relation to the protection of that information, as more particularly set forth in 45 C.F.R. § 164.308.

(e) **Breach**. Means the unauthorized acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E, Part 164 of the HIPAA Privacy Rule, which compromises the security or privacy of the protected health information. Breach **excludes**:

- 1) any unintentional acquisition, access, or use of protected health information by a workforce member or person, acting under the authority of the Business Associate, if
  - a) such acquisition, access, or use was made in good faith and within the course and scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of the HIPAA Privacy Rule.
- 2) Any inadvertent disclosure by a person who is authorized to access protected health information at the Business Associate to another person authorized to access protected health information at the same Business Associate or Organized Health Care Arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of the HIPAA Privacy Rule.
- 3) A disclosure of protected health information where a Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made was not reasonably able to have retained such information.

Except as provided in paragraphs 1-3 of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.

(f) **Physical Safeguards**. Means physical measures, policies, and procedures to protect Business Associate's information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion, as more particularly set forth in 45 C.F.R. § 164.310.

(g) **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. It may or may not include a breach of PHI.

(h) **Technical Safeguards**. Means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it, as more particularly set forth in 45 C.F.R. § 164.312.

(i) **Unsecured Protected Health Information**. Means any PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

(j) **Destruction of PHI**. Means the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals when disposing of PHI.

All other terms used herein that are not specifically defined above shall have the same meanings as those terms defined in 45 C.F.R. Parts 160 and 164. Said terms and definitions set forth therein are incorporated herein by reference.

### **3. Privacy Rule Obligations and Activities of Business Associate**

(a) Business Associate agrees not to use or disclose PHI other than to perform its duties as stated in this Agreement, or as required by law.

(b) Business Associate agrees to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 to prevent use or disclosure of the PHI other than as provided for in this Agreement. Business Associate ensures that it has policies and procedures that ensure that appropriate and adequate safeguards are in place to prevent improper use or disclosure of PHI.

(c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

(d) Business Associate agrees to report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware. The Business Associate shall report the incident as soon as possible, but in no case later than ten calendar days from the date the incident is known to the Business Associate.

(e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created, maintained, or received by Business Associate on behalf of Covered Entity, agrees in writing to the same restrictions, conditions, and requirements that apply through this Agreement to Business Associate with respect to such information.

(f) Business Associate agrees to provide access, at the request of Covered Entity, and in a prompt and timely manner, to PHI in a Designated Record Set to Covered Entity or, as directed by Covered Entity to an Individual in order to meet the requirements of 45 C.F.R. § 164.524.

(g) Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of the Covered Entity or an Individual.

(h) Business Associate agrees to make its internal practices, books, and records, including policies and procedures relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to the Covered Entity, or to the Secretary, in a prompt and timely manner or as designated by the Secretary, for purposes of determining Covered Entity's compliance with the Privacy Rule.

(i) Business Associate agrees to document such disclosures of PHI as would be required for Covered Entity to respond timely to a request by an Individual for an accounting of disclosures of PHI and provide in a prompt and timely manner any information related to such disclosures in accordance with 45 C.F.R. § 164.528. This would include any unintentional or inadvertent disclosures that constitute a Breach. Business Associate agrees to keep records of the accounting of a disclosure for six (6) years.

(j) Business Associate shall require any agent or subcontractor to whom it provides Covered Entity's PHI to enter into a written agreement between Business Associate and such agent or subcontractor substantially identical to this Agreement, and obligating such agents and subcontractors to the same restrictions on use and disclosure of PHI as are imposed up Business Associate in this Agreement. Business Associate shall furnish evidence to Covered Entity of the execution of such an agreement by its agents or subcontractors before furnishing PHI to such entities.

(k) Business Associate agrees that, in requesting PHI from Covered Entity, and in using or disclosing PHI to others, only the Minimum Necessary information shall be requested, used, or disclosed.

(l) Business Associate agrees to educate the members of its workforce concerning HIPAA Privacy, including policies and procedures related to this agreement, and to provide proof of that education upon the request of the Secretary and/or the Covered Entity.

(m) Business Associate agrees to meet the Privacy/Security and ARRA HITECH provisions for the destruction of PHI when such destruction is necessary. Business Associate shall implement and maintain

data retention and data destruction policies and procedures that ensure the security of the PHI. Such policies and procedures must be made available to the Covered Entity at the Covered Entity's request.

(n) To the extent the Business Associate is to carry out one or more of the Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).

#### **4. Security Rule Obligations of Business Associate and Breach Notification**

(a) Business Associate agrees to implement and document, as set forth in 45 C.F.R. § 164.316, Administrative Safeguards, Physical Safeguards, and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic, physical, and verbal PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity. In addition, Business Associate agrees to, in accordance with the requirements of 45 C.F.R. Part 164, Subpart C, and specifically, but not exclusively

1. Ensure the confidentiality, integrity, and availability of all PHI the Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Regulations;

(b) Business Associate agrees to ensure that any agent or subcontractor, to whom Business Associate provides this information agrees to implement and document reasonable and appropriate Administrative Safeguards, Physical Safeguards, and Technical safeguards, including at least the requirements set forth in this Section for Business Associate;

(c) Business Associate agrees to report to Covered Entity any Security Incident which puts Covered Entity's PHI at risk of unauthorized disclosure or Breach of unsecured PHI of which Business Associate has knowledge.

For purposes of this section, a Breach or Security Incident shall be treated as discovered by a Business Associate as of the first day on which the Breach or Security Incident is known to the Business Associate, or by exercising reasonable diligence, would have been known to the Business Associate. A Business Associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the Business Associate.

Business Associate shall, following the discovery of a Breach or Security Incident of such information notify Covered Entity immediately and in no case later than ten (10) calendar days after discovery of the Breach or Security Incident, except as provided in 45 C.F.R. §164.412.

In the event of a Breach or Security Incident, Business Associate shall notify Covered Entity and include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been accessed, acquired, used, or disclosed during the Breach.

The Business Associate shall provide the Covered Entity with any other available information that the Covered Entity is required to include in the notification of the Individual under §164.404(c) at the time of the notification or as promptly thereafter as information becomes available.

The Business Associate will report any Breach or Security Incident to the Covered Entity's "Privacy Officer". In the event that the Privacy Officer cannot be contacted, the Hospital Administrator shall be contacted.

It is understood that the Covered Entity will make the necessary disclosure to the Individual and the Secretary, as required by law; however, Business Associate shall be responsible for any and all costs and expenses associated with a Breach committed by Business Associate, including but not limited to, fines, penalties, and direct costs associated with notification of the Secretary and the Individual(s) whose PHI has been breached."

(d) Business Associate agrees to make its policies and procedures, and documentation required by this Section relating to safeguards and breach reporting available, if requested, to the Secretary and to Covered Entity for purposes of determining the Business Associate's compliance with this Section;

(e) Business Associate agrees to educate the members of its workforce concerning the requirements of HIPAA Security and Breach Notification, and will provide proof of that education upon the request of the Secretary and/or the Covered Entity;

(f) Business Associate authorizes termination of the Contract or other relationship by Covered Entity if Covered Entity determines that the Business Associate has violated a material term of the Contract or this Agreement.

#### **5. Permitted Uses and Disclosures by Business Associate**

(a) Except as otherwise prohibited by law or limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in this Agreement or intended by the parties, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity or the Privacy Rule, including, but not limited to the following:

- (1) Use or disclose PHI for proper management and administration to carry out the legal responsibilities of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential 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 the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached. Entities to which Business Associate discloses PHI for the purpose of management and administration of the Business Associate shall be deemed "agents" or "subcontractors" of Business Associate, within the meaning of Section 3(e) of this Agreement.
- (2) Use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e) (2) (i) (B) (2) (i).

#### **6. Obligations of Covered Entity**

(a) Covered Entity shall notify Business Associate of any limitation(s) in its Notice of Privacy Practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI. Business Associate acknowledges that it has received a copy of Covered Entity's Notice of Privacy Practices, and agrees to comply with all limitations on use and disclosure of PHI contained therein.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(c) Covered Entity shall notify Business Associate of any changes in Covered Entity's Notice of Privacy Practices.

## **7. Term - and Termination of Agreement**

(a) Term. The Term of this Agreement shall be effective as of the date of execution by the last party executing same, 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.

(b) Termination for Cause. Notwithstanding any other provisions of this Agreement, upon Covered Entity's knowledge of a material breach by Business Associate of the terms of this Agreement, Covered Entity shall either:

- (1) Provide an opportunity for Business Associate to cure the breach. Covered Entity may terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
- (2) Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or
- (3) If neither termination nor cure is feasible in the sole discretion of Covered Entity, Covered Entity shall report the violation to the Secretary.

(c) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. Business Associate shall not retain copies of any PHI. This provision shall also apply to PHI: that is in the possession of subcontractors or agents of Business Associate.

(2) In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall notify Covered Entity of this determination and its reasons. If Covered Entity agrees that return or destruction of PHI is not feasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures, for so long as Business Associate maintains such PHI. This provision shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate.

## **8. Miscellaneous**

(a) Regulatory References. Any reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

(b) Formal Amendment and Deemed Amendment. The Parties agree to take such action as is necessary to formally amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191. Regardless of the execution of a formal amendment of this Agreement, the Agreement shall be deemed amended to permit the Covered Entity to comply with HIPAA and the Privacy Rule, as the same may be hereafter amended or interpreted.

(c) Survival. The respective rights and obligations of Business Associate under Section 7 (c) of this Agreement entitled "Effect of Termination" shall survive the termination of this Agreement and/or the Agreement.

(d) Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

(e) Material Breach of Agreement as Breach of Contract. Any material breach of this Agreement by Business Associate shall constitute a material breach of the Contract, and shall entitle Covered Entity to any of the remedies provided in the Contract, in addition to the remedies provided herein.

(f) Provisions of Agreement to Control. In the event of any conflict between the provisions of this Agreement and any of the other provisions of the Contract, including any renewal, extension or modification thereof, the provisions of this Agreement shall control.

(g) Ownership of PHI. The PHI to which Business Associate, or any agent or subcontractor of Business Associate has access under the Agreement shall be and remain the property of Covered Entity.

(h) Indemnification and Contribution. Each party to this Agreement shall indemnify and hold the other harmless from any and all claims, liability, damages, costs and expenses, including attorney's fees and costs of defense and attorney's fees, resulting from the action or omission of the other party. In the event that any liability, damages, costs and expenses arise as a result of the actions or omissions of both parties, each party shall bear such proportion of such liability, damages, costs and expenses as are attributable to the acts or omissions of such party.

(i) Injunctive Relief. Notwithstanding any rights or remedies provided for in this Agreement, Covered Entity retains all rights to seek injunctive relief to prevent or stop the inappropriate use or disclosure of PHI directly or indirectly by Business Associate, or any agent or subcontractor of Business Associate.

(j) Attorney's Fees. If any legal action or other proceeding is brought for the enforcement of this Agreement or in connection with any of its provisions, the prevailing party shall be entitled to an award for the attorney's fees and costs incurred therein in addition to any other right of recovery.

(k) Severability. If any clause or provision of this Agreement is held to be illegal, invalid or unenforceable under any present or future law, the remainder of this Agreement will not be affected thereby. It is the intention of the parties that, if any such provision is held to be illegal, invalid or unenforceable, there will be substituted in lieu thereof a provision as similar in terms to such provision as is possible which is legal, valid and enforceable.

(l) Waiver of Provisions. Failure by either party at any time to enforce or require the strict performance of any of the terms and conditions of this Agreement shall not constitute a waiver or such terms or conditions or modify such provision or in any manner render it unenforceable as to any other time or as to any other occurrence. Any specific waiver by either party of any of the terms and conditions of this Agreement shall be considered a one-time event and shall not constitute a continuing waiver. Neither a waiver nor any failure to enforce shall in any way affect or impair the terms or conditions of this Agreement or the right of either party to avail itself of its remedies.

(m) Choice of Law. To the extent not preempted by HIPAA or the Privacy Rule, the Laws of the State of Louisiana shall govern this Agreement.

(n) Notices. Any notice, demand or communication required or permitted to be given by any provision of this Agreement shall be in writing and will be deemed to have been given when actually delivered (by whatever means) to the party designated to receive such notice, or on the next business day following the day sent by overnight courier, or on the third (3rd) business day after the same is sent by certified United States mail, postage and charges prepaid, directed to the addresses noted below, or to

such other or additional address as any party might designate by written notice to the other party, whichever is earlier.

(o) Attestation of Compliance. The signature of the Business Associate to this Agreement indicates compliance to the requirements outlined in this Agreement.

Notices required by this Agreement shall be sent as follows:

Covered Entity:

Business Associate:

[Name]  
[Institution]  
[Address]  
[City, State, Zip Code]

[Name]  
[Institution]  
[Address]  
[City,State,Zip Code]

Copy to:

Copy to:

[Name]  
[Institution]  
[Address]  
[City,State,Zip Code]

[Name]  
[Institution]  
[Address]  
[City,State,Zip Code]

THUS DONE AND SIGNED on the date first written above:

**[Name of Covered Entity]**

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

Title:

**[Name of Business Associate]**

\_\_\_\_\_



By:

Title:

**Facility Privacy Officer Contact Information**

**Privacy Officer:**

**Contact Phone Number(s):**

**Contact Address:**