

## **HIPAA BUSINESS ASSOCIATE AGREEMENT**

This BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is entered into by and between DIVERSIFIED HEALTH CARE MANAGEMENT, INC. (the "Business Associate"), and \_\_\_\_\_ (the "Covered Entity") (collectively referred to herein as the "Parties" or individually as a "Party"), to be effective as of the \_\_\_ day of \_\_\_\_\_, 20\_\_ (the "Effective Date"), and is made a part of that certain service agreement or service agreements between the Parties (the "Service Agreement").

WHEREAS, Covered Entity has a business relationship with Business Associate that is memorialized in the Service Agreement pursuant to which Business Associate may be considered a "Business Associate" of Covered Entity as defined in the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as codified at 42 U.S.C. § 1320d ("HIPAA"), including all pertinent regulations set forth in Title 45, Parts 160 and 164 of the Code of Federal Regulations ("C.F.R.") issued by the U.S. Department of Health and Human Services as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act of 2009, as codified at 42 U.S.C.A. prec. § 17901 (the "HITECH Act"), part of the American Recovery and Reinvestment Act of 2009 ("ARRA"), 42 U.S.C. §§ 17921, 17931-17932 and 17934; and

WHEREAS, the nature of the contractual relationship between Covered Entity and Business Associate involves the use and/or disclosure of Protected Health Information ("PHI") as that term is defined in 45 C.F. R. 160.103; and

WHEREAS, for good and lawful consideration as set forth in the Service Agreement, Covered Entity and Business Associate enter into this Agreement for the purpose of ensuring compliance with the requirements of HIPAA, its implementing regulations, the HITECH Act and any current and future regulations promulgated under HIPAA or HITECH Act (HIPAA, HITECH Act and any current and future regulations promulgated under either are hereinafter referred to as the "Regulations").

NOW THEREFORE, in consideration of the mutual covenants contained herein which are made a contractual part hereof and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

**1. Definitions.** Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in the Regulations, including without limitation, the Privacy Rule, as set forth in the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E, as amended by the HITECH Act and as may otherwise be amended from time to time.

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

Except as otherwise limited in the Service Agreement and/or 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, provided that such use or disclosure would not violate the Privacy Rule or the HITECH Act if done by Covered Entity as specified in this Agreement or the minimum necessary policies and procedures of the Covered Entity, as follows:

- **Permitted Uses.** Except as otherwise limited in this Agreement or as Required by Law, Business Associate may use PHI as necessary for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.
- **Data Aggregation.** Except as otherwise limited in this Agreement, Business Associate may use PHI to provide data aggregation services to Covered Entity as permitted by 45 CFR §164.504(e)(2)(i)(B), to the extent specifically required under the Agreement;

- Re-creation of Information. Except as otherwise limited in this Agreement, Business Associate may use PHI received or created pursuant to this Agreement to create information that is not individually identifiable health information (“De-identified Information”), consistent with the standards set forth at 45 C.F.R. § 164.514.
- Permitted Disclosures. Business Associate shall not disclose PHI except for the purpose of performing the Business Associate’s obligations under the Service Agreement or this Agreement. Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable written assurances from the person to whom the PHI is disclosed that (1) the PHI will be held confidentially as provided pursuant to this Agreement and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person; and (2) Business Associate will be notified within 24 hours of the discovery of any breach or suspected breach of the confidentiality of the PHI.

**3. Prohibited Uses and Disclosures by Business Associate.**

- Business Associate shall not use or disclose PHI for marketing purposes or any other purpose not permitted by this Agreement, the Service Agreement or the Privacy Rule or HITECH Act.
- Business Associate shall not disclose PHI to a health plan for payment or health care operations purposes if the individual patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates as required by 42 U.S.C. § 17935(a).
- Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of Covered Entity and as permitted by the HITECH Act, as described in 42 U.S.C. § 17935(d)(2); however, this prohibition shall not affect payment by Covered Entity to Business Associate for services provided pursuant to the Service Agreement.

**4. Obligations and Activities of Business Associate. Business Associate covenants and agrees to the following:**

- Compliance. Business Associate shall be directly responsible for full compliance with the relevant requirements of both the HIPAA Privacy Rule and Security Rule.
- Appropriate Safeguards. Business Associate shall implement and maintain reasonable and appropriate safeguards as are necessary to prevent the use, disclosure or availability of PHI or electronic PHI that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity, other than as permitted by the Service Agreement or this Agreement, including, but not limited to, administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI in accordance with 45 C.F.R. §§ 164.308, 164.310 and 164.312. Business Associate shall comply with the policies and procedures and documentations requirements of the HIPAA Security Rule, including but not limited to, 45 C.F.R. § 164.316 and the HITECH Act, 42 U.S.C. § 17931.
- Designated Security Officer. Business Associate shall designate an individual to serve as the Security Officer responsible for supervising the security and privacy mechanisms, including but not limited to, administrative, physical and electronic mechanisms employed within the organization to prevent unauthorized use, disclosure or access to PHI maintained by Business Associate on behalf of Covered Entity.
- Business Associate’s Agents. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. This provision shall not, however, be deemed to provide Business Associate with a right to assign or subcontract its responsibilities, except as specifically provided in the Service Agreement. In the event Business Associate creates, maintains, receives or transmits electronic PHI on behalf of Covered Entity, Business Associate shall implement the safeguards required by Section 4.b. above with respect to electronic PHI.

- Duties of Business Associate Involving Breach or Unauthorized Access, Use or Disclosure of PHI.
  - Discovery of Breaches. A Breach shall be treated as discovered by Business Associate as of the first day on which such Breach is known to the Business Associate, 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 Business Associate (determined in accordance with the federal common law of agency).
  - Notification. Business Associate shall notify the designated Privacy Official of Covered Entity within five (5) business days after discovery of any access, use or disclosure of PHI not permitted by this Agreement or the Service Agreement, any security incident involving electronic PHI and any Breach of Unsecured PHI of which Business Associate becomes aware and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. Business Associate shall take any prompt corrective action to cure any such deficiencies and any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.
  - Reporting Improper Access, Use or Disclosure. Business Associate shall provide the following information to Covered Entity within ten (10) business days of discovery of a Breach except when, despite all reasonable efforts of Business Associate to obtain the information required, circumstances beyond the control of the Business Associate necessitate additional time. Under such circumstances, Business Associate shall provide to Covered Entity the following information as soon as possible and without unreasonable delay, but in no event later than forty-five (45) calendar days from the date of discovery of a Breach:
    - the date of the breach;
    - the date of the discovery of the breach;
    - a general description of events leading up to and surrounding the breach;
    - a description of the types of unsecured PHI that were involved;
    - a listing of the identification of each individual and/or class of individuals whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired or disclosed; and
    - any other details necessary to complete an assessment of the risk of harm to the individual.

Business Associate shall provide the designated Privacy Official of Covered Entity with updates of information concerning the details of such Breach and the final results of its Risk Assessment as required in Section 4.e.(4) as needed to ensure that such information remains current.

- Risk Assessment and Investigation. Business Associate shall perform an appropriate risk assessment immediately following the discovery of any unauthorized access, use or disclosure of PHI to determine whether use, access, or disclosure is one that “poses a significant risk of financial, reputation or other harm to the individual.” In performing the Risk Assessment, Business Associate should consider a combination of factors such as: (a) who impermissibly used the PHI or to whom the PHI was impermissibly disclosed; (b) was the impermissibly disclosed PHI returned prior to it being accessed for an improper purpose; and (c) the type and amount of PHI involved in the impermissible use or disclosure.

The results of such Risk Assessment shall be provided to Covered Entity in writing, without unreasonable delay and in no event later than thirty (30) days from the date of discovery of the unauthorized access, use or disclosure. In addition to the Risk Assessment conducted by the Business Associate, Covered Entity reserves the right to conduct its own investigation of any unauthorized access, use or disclosure of PHI occurring at any facility, site or location of Business Associate, its agents or subcontractors or

through any systems under the control of the Business Associate, its agents or subcontractors. Business Associate shall cooperate with Covered Entity to conduct such investigation. Covered Entity agrees to provide advance notice of such investigation, to protect the confidentiality of and not disclose any confidential and proprietary information of Business Associate to which Covered Entity has access during the course of such investigation.

- Mitigation of Harm. In the event of a Breach of Unsecured PHI, Business Associate agrees to maintain adequate procedures for mitigating, to the extent practicable, any harmful effects of a system compromise or other improper use or disclosure of PHI maintained by Business Associate, such as promptly obtaining reasonable assurance from the recipient that the information will not be further used or disclosed in a confidentiality agreement or will be destroyed.
- Notification to Individual. It is the sole responsibility of the Covered Entity to notify individual patients/customers of any Breach of PHI. At no time, is Business Associate to contact or speak directly with any of Covered Entity's individual patients/customers who are the subject of any Breach of PHI. Any such inquiries should be directed to the Covered Entity's Privacy Officer. Business Associate shall cooperate with Covered Entity as necessary to provide such notification and any details pertaining to any Breach of PHI.
- Cooperation with Law Enforcement. Business Associate shall cooperate with Covered Entity in the event law enforcement officials institute an investigation that involves a Breach of PHI under this Agreement.
- Notification to Media. For a Breach of PHI involving more than 500 individuals, it is solely the responsibility of Covered Entity to notify the media and appropriate law enforcement and federal and State agencies as required by the HITECH Act, 45 C.F.R. 164.406. At no time is Business Associate to contact or speak directly with the media without the prior authorization of Covered Entity. Business Associate shall cooperate with Covered Entity as necessary to provide such notification to the media.
- Access to PHI. Upon reasonable notice and prior written request from Covered Entity, Business Associate agrees to provide access to PHI in a Designated Record Set to Covered Entity, or to provide access to PHI to an Individual pursuant to a customer's right of access to obtain a copy of his or her PHI under 45 C.F.R. §164.524.
- Governmental Access to Records. Upon reasonable notice and prior written request, Business Associate agrees to make available during normal business hours at Business Associate's offices all internal practices, books, records, agreements, policies and procedures relating to the use of and disclosure of PHI, created or received by Business Associate on behalf of Covered Entity, available to the Covered Entity, or to the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- Minimum Necessary. Business Associate shall request, use and disclose only the minimum amount of PHI necessary to accomplish the purposes of the request, use or disclosure in the Service Agreement. The Minimum Amount of PHI shall mean the minimum necessary as meant by the intended language of the HITECH Act.
- Amendments of PHI. If, and to the extent that Business Associate possesses an applicable Designated Record Set, within a reasonable amount of time of receipt of a request from the Covered Entity for the amendment of an Individual's PHI contained in the Designated Record Set, Business Associate agrees to provide such information to Covered Entity for amendment and shall also incorporate any such amendments in the PHI maintained by Business Associate as required by 45 C.F.R. § 164.526.
- Accounting Rights. Business Associate and its agents or subcontractors shall make available to Covered Entity the information required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations under the Privacy Rule and the HITECH Act. Business Associate agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request, unless the Regulations allow for a shorter period. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received the PHI and if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a

copy of the individual's authorization or a copy of the written request for disclosure. Business Associate is expected to meet the requirements described in this Section 4.j. with respect to Electronic Health Records by the Compliance Date as set forth in the HITECH Act of February 17, 2010.

**5. Continuing Obligations/Termination.** During the term of the Agreement, Business Associate covenants and agrees that it shall:

- **Term.** The Obligations of Business Associate set forth herein shall commence on the Effective Date and shall terminate when the Agreement terminates and all of the PHI 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 PHI, the terms of this Agreement are extended to cover such information and survive termination of this Agreement.
- **Termination for Cause.** Upon Covered Entity's knowledge of a material breach by Business Associate to the terms of this Agreement, Covered Entity may terminate this Agreement, and sever all business relationships with Business Associate, including the termination of the Service Agreement and any and all Agreements with Business Associate if the breach remains uncured for more than fifteen (15) days after Covered Entity gives written notice to Business Associate of the breach. The effective date of such termination will be the 16<sup>th</sup> day from the date of the written notice of breach.
- **Immediate Termination.** In the event Business Associate has breached a material term of this Agreement and cure is not possible, Covered Entity may immediately terminate this Agreement, and sever all business relationships with Business Associate, including the termination of the Service Agreement and any and all Agreements with Business Associate. Covered Entity may report such violation to the Secretary.
- **Effect of Termination.**
  - Except as provided in this Section 5.d. of this Agreement, upon termination of this Agreement for any reason, Business Associate shall return or destroy all PHI created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.
  - In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Business Associate 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 Business Associate maintains such PHI.
  - The provisions of this Section 5.d. shall survive termination of this Agreement.

**6. Obligations of Covered Entity to Inform Business Associate of Privacy Practices and Individual Restrictions.**

- **Notice of Privacy Practices.** Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 C.F.R. §164.406, as well as any changes to such notice. Any notices given hereunder shall be in writing and addresses as follows:

Diversified Health Care Management, Inc.  
P.O. Box 241769  
Anchorage, AK 99524-1769

- **Changes in Permitted Uses.** Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures.

- Restrictions on Use. Covered Entity shall notify Business Entity of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. §164.406

## **7. Indemnification.**

- **Business Associate Indemnity.** Business Associate hereby agrees to indemnify and hold harmless Covered Entity and its respective parent corporation and subsidiaries, their directors, officers, subcontractors, agents, servants and employees (collectively, the "Covered Entity Indemnitees") to the extent any claims, causes of action, liabilities, judgments, fines, assessments, penalties, damages, awards or other expenses of any kind or nature whatsoever, including, without limitation, reasonable attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution to which the Covered Entity Indemnitees may become subject as the result of any: (i) breach of this Agreement by Business Associate; (ii) failure of Business Associate to perform its obligations hereunder; (iii) negligence or legal fault of Business Associate, its directors, officers, agents or employees; or (iv) violation of the Regulations by Business Associate.
- **Covered Entity Indemnity.** Covered Entity hereby agrees to indemnify and hold harmless Business Associate and its respective parent corporation and subsidiaries, their directors, officers, subcontractors, agents, servants and employees (collectively, the "Business Associate Indemnitees") to the extent any claims, causes of action, liabilities, judgments, fines, assessments, penalties, damages, awards or other expenses of any kind or nature whatsoever, including, without limitation, reasonable attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution to which the Business Associate Indemnitees may become subject as the result of any: (i) breach of this Agreement by Covered Entity; (ii) failure of Covered Entity to perform its obligations hereunder; (iii) negligence or legal fault of Covered Entity, its directors, officers, agents or employees; or (iv) violation of the Regulations by Covered Entity.

## **8. General Provisions.**

- Regulatory References. A reference in this Agreement to a section in the Privacy Rule, Security Rule and HITECH Act means that section as in effect or as amended.
- Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for either Covered Entity or Business Associate to comply with all federal, state and local laws and regulations, including, but not limited to, the requirements of the Privacy Rule, HIPAA and the HITECH Act. This Agreement shall be changed, modified or amended only by an instrument in writing signed by a duly authorized representative of each of the Parties, effective as of the date stipulated therein and attached hereto.
- Survival. The respective rights and obligations of Business Associate and Covered Entity set forth in Sections 3, 4, 5.d., 7 and 8 shall survive the termination of this Agreement.
- Interpretation. Should there be any conflict between the language of this Agreement and any other Agreement entered into between the Parties, the language and provisions of this Agreement shall control and prevail unless the Parties specifically refer in a subsequent written agreement to this Agreement by its title and date and specifically state that the provisions of the later written agreement shall control over this Agreement.
- Notices. Any notices required or permitted hereunder shall be sufficiently given if sent by registered or certified mail, postage prepaid, or personally delivered, addressed or delivered to the addresses set forth below in the signatures to this Agreement or to such other addresses as shall be furnished in writing by either party to the other party; and any such notice shall be deemed to have been given, if mailed, as of the date mailed, and, if personally delivered, as of the date delivered. Notices pertaining to unauthorized use or access of PHI or Breaches of PHI should be submitted to the Covered Entity's Compliance and/or Privacy Officer with contact information of Business Associate's designated Security Official responsible for investigating such incidents.
- Facsimile. The signature of any party on this Agreement, or any subsequent amendment thereto, transmitted by way of a facsimile machine shall be considered for all purposes as an original signature. Any such faxed Agreement or amendment shall be considered to have the same binding legal effect as an original Agreement or

**Diversified Health Care Management, Inc.**

amendment. At the request of any party, the faxed Agreement or amendment shall be re-executed by each signatory party in an original form.

- Entire Agreement. With regard to the subject matter herein, this Agreement supersedes prior or contemporaneous discussions, agreements, understandings, and representations between the Covered Entity and Business Associate.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be executed by its duly authorized representative as of the date first above written.

**COVERED ENTITY**

**Signature**

**Date**

**Name / Title (PLEASE PRINT)**

**Mailing Address**

**City State Zip Code**

**Phone #:**

**Fax #:**

**Email Address**

**Diversified Health Care Management, INC (DHCM)**

**By:** \_\_\_\_\_  
**Joseph E. Beaty, CEO**

**Address:** 4141 B Street  
Suite 401  
Anchorage, AK 99503

**Phone:** 907- 770-2380

**Date:** \_\_\_\_\_

**Fax:** 907- 770-2341