

## BUSINESS ASSOCIATE AGREEMENT

### SECTION 1: DEFINITIONS

“**Breach**” shall have the same meaning given to such term in 42 U.S.C. § 17921(1) and 45 C.F.R. § 164.402.

“**Designated Record Set**” shall have the same meaning as the term “designated record set” in 45 C.F.R. § 164.501.

“**Electronic Health Record**” shall have same meaning given to such term in 42 U.S.C. § 17921(5).

“**Electronic Protected Health Information**” or “**Electronic PHI**” shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. § 160.103, as applied to the information that CompuHealth Northwest creates, receives, maintains or transmits from or on behalf of Customer.

“**Individual**” shall have the same meaning as the term “individual” in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

“**Privacy Rule**” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 162 and Part 164, Subparts A and E.

“**Protected Health Information**” or “**PHI**” shall have the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, as applied to the information created or received by CompuHealth Northwest from or on behalf of Customer.

“**Required by Law**” shall have the same meaning as the term “required by law” in 45 C.F.R. § 164.103.

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

“**Security Incident**” shall have the meaning given to such term in 45 C.F.R. § 164.304, but shall not include, (a) unsuccessful attempts to penetrate computer networks or servers maintained by CompuHealth Northwest and (b) immaterial incidents that occur on a routine basis, such as general “pinging” or “denial of service” attacks.

“**Security Rule**” shall mean the Security Standards at 45 C.F.R. Parts 160 and 162 and Part 164, Subparts A and C.

“**Unsecured PHI**” shall have the same meaning given to such term under 42 U.S.C. § 17931(h), and guidance promulgated thereunder.

Capitalized Terms. Capitalized terms used in this BAA and not otherwise defined herein shall have the meanings set forth in the Privacy Rule, the Security Rule, and the HITECH Act, which definitions are incorporated in this BAA by reference.

### SECTION 2: PERMITTED USES AND DISCLOSURES OF PHI

2.1 Uses and Disclosures of PHI Pursuant to Agreement. Except as otherwise limited in this BAA, CompuHealth Northwest may use or disclose PHI to perform functions, activities or services for, or on behalf of, Customer as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Customer.

2.2 Permitted Uses of PHI by CompuHealth Northwest. Except as otherwise limited in this BAA, CompuHealth Northwest may use PHI for the proper management and administration of CompuHealth Northwest or to carry out the legal responsibilities of CompuHealth Northwest.

2.3 Permitted Disclosures of PHI by CompuHealth Northwest. Except as otherwise limited in this BAA, CompuHealth Northwest may disclose PHI for the proper management and administration of CompuHealth Northwest, provided that the disclosures are Required by Law, or CompuHealth Northwest obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person (which purpose must be consistent with the limitations imposed upon CompuHealth Northwest pursuant to this BAA), and that the person agrees to notify CompuHealth Northwest of any instances of which it is aware in which the confidentiality of the information has been breached. CompuHealth Northwest may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).

2.4 Data Aggregation. Except as otherwise limited in this BAA, CompuHealth Northwest may use PHI to provide Data Aggregation services as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B), including use of PHI for statistical compilations, reports, research and all other purposes allowed under applicable law.

2.5 De-identified Data. CompuHealth Northwest may create de-identified PHI in accordance with the standards set forth in 45 C.F.R. § 164.514(b) and may use or disclose such de-identified data for any purpose.

2.6 Disclosure Pursuant to Authorization. Without limiting the generality of the foregoing, CompuHealth Northwest reserves the right at its sole discretion to disclose an Individual's PHI in response to and in accordance with a valid authorization executed by such individual that meets the requirements set forth in the Privacy Rule.

### **SECTION 3: OBLIGATIONS OF COMPUHEALTH NORTHWEST**

#### **3.1 Appropriate Safeguards.**

3.1.1 Privacy of PHI. CompuHealth Northwest will use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the Agreement and this BAA. The safeguards must reasonably protect PHI from any intentional or unintentional use or disclosure in violation of the Privacy Rule and this BAA, and limit incidental uses or disclosures made pursuant to a use or disclosure otherwise permitted by this BAA.

3.1.2. Security of PHI. CompuHealth Northwest will use appropriate administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI, as required by the Security Rule. CompuHealth Northwest will comply with the provisions of 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316 relating to implementation of administrative, physical and technical safeguards with respect to Electronic PHI in the same manner that such provisions apply to a HIPAA covered entity. CompuHealth Northwest will also comply with any additional security requirements contained in the HITECH Act that are applicable to a business associate.

3.2 Reporting of Improper Use or Disclosure, Security Incident or Breach. CompuHealth Northwest will report to Customer any use or disclosure of PHI not provided for by the Agreement of which it becomes aware. CompuHealth Northwest will report to Customer any Security Incident of which it becomes aware. CompuHealth Northwest will notify Customer of any Breach of Unsecured PHI as soon as practicable, and no later than 30 days after discovery of such Breach. CompuHealth Northwest's notification to Customer of a Breach will include: (a) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by CompuHealth Northwest to have been, accessed, acquired or disclosed during the Breach; and (b) any particulars regarding the Breach that Customer would need to include in its notification, as such particulars are identified in 42 U.S.C. § 17932 and 45 C.F.R. § 164.404.

3.3 CompuHealth Northwest's Agents. CompuHealth Northwest will ensure that any agent or subcontractor to whom it provides PHI received from, or created or received by CompuHealth Northwest on behalf of Customer, agrees to restrictions and conditions that are substantially similar to those that apply through this BAA to CompuHealth Northwest with respect to such PHI. CompuHealth Northwest will ensure that any agent, including a subcontractor, to whom it provides Electronic PHI agrees to implement reasonable and appropriate safeguards to protect such information.

3.4 Access to PHI. The parties do not intend for CompuHealth Northwest to maintain any PHI in a Designated Record Set for Customer. To the extent CompuHealth Northwest possesses PHI in a Designated Record Set, CompuHealth Northwest agrees to make such information available to Customer pursuant to 45 C.F.R. § 164.524 and 42 U.S.C. § 17935(e)(1), as applicable, within ten business days of CompuHealth Northwest's receipt of a written request from Customer; provided, however, that CompuHealth Northwest is not required to provide such access where the PHI contained in a Designated Record Set is duplicative of the PHI contained in a Designated Record Set possessed by Customer. If an Individual makes a request for access pursuant to 45 C.F.R. § 164.524 directly to CompuHealth Northwest, or inquires about his or her right to access, CompuHealth Northwest will direct the Individual to Customer.

3.5 Amendment of PHI. The parties do not intend for CompuHealth Northwest to maintain any PHI in a Designated Record Set for Customer. To the extent CompuHealth Northwest possesses PHI in a Designated Record Set, CompuHealth Northwest agrees to make such information available to Customer for amendment pursuant to 45 C.F.R. § 164.526 within 20 business days of CompuHealth Northwest's receipt of a written request from Customer. If an Individual submits a written request for amendment pursuant to 45 C.F.R. § 164.526 directly to CompuHealth Northwest, or inquires about his or her right to amendment, CompuHealth Northwest will direct the Individual to Customer.

3.6 Documentation of Disclosures. CompuHealth Northwest agrees to document such disclosures of PHI and information related to such disclosures as would be required for Customer to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528, and 42 U.S.C. § 17935(c), as applicable. CompuHealth Northwest will document, at a minimum, the following information ("Disclosure Information"): (a) the date of the disclosure; (b) the name and, if known, the address of the recipient of the PHI; (c) a brief description of the PHI disclosed; (d) the purpose of the disclosure that includes an explanation of the basis for such disclosure; and (e) any additional information required under the HITECH Act and any implementing regulations.

3.7 Accounting of Disclosures. CompuHealth Northwest agrees to provide to Customer, within 20 business days of CompuHealth Northwest's receipt of a written request from Customer, information collected in accordance with Section 3.6 of this BAA, to permit Customer to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528, and 42 U.S.C. § 17935(c), as applicable.

3.8 Governmental Access to Records. CompuHealth Northwest will make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by CompuHealth Northwest on behalf of, Customer available to the Secretary for purposes of the Secretary determining Customer's compliance with the Privacy Rule and the Security Rule.

3.9 Mitigation. To the extent practicable, CompuHealth Northwest will cooperate with Customer's efforts to mitigate a harmful effect that is known to CompuHealth Northwest of a use or disclosure of PHI not provided for in this BAA.

3.10 Minimum Necessary. CompuHealth Northwest will request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure, in accordance with 42 U.S.C. § 17935(b) and regulations promulgated thereunder.

3.11 Limitation on Marketing. CompuHealth Northwest may use and disclose PHI for marketing purposes only as expressly directed by Customer, and in accordance with 42 U.S.C. § 17936(a). CompuHealth Northwest will not use or disclose PHI for fundraising purposes.

3.12 Limitation on Sale of Electronic Health Records and PHI. CompuHealth Northwest will comply with the prohibition on the sale of Electronic Health Records and PHI set forth in 42 U.S.C. § 17935(d).

3.13 HITECH Act Applicability. CompuHealth Northwest acknowledges that enactment of the HITECH Act amended certain provisions of HIPAA in ways that now directly regulate, or will on future dates directly regulate, CompuHealth Northwest under the Privacy Rule and Security Rule. To the extent not referenced or incorporated

herein, requirements applicable to CompuHealth Northwest under the HITECH Act are hereby incorporated by reference into this BAA. CompuHealth Northwest agrees to comply with applicable requirements imposed under the HITECH Act, as of the effective date of each such requirement.

#### **SECTION 4: OBLIGATIONS OF CUSTOMER**

4.1 Notice of Privacy Practices. Customer will notify CompuHealth Northwest 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 CompuHealth Northwest's use or disclosure of PHI. Customer will provide such notice no later than 15 days prior to the effective date of the limitation.

4.2 Notification of Changes Regarding Individual Permission. Customer will notify CompuHealth Northwest of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect CompuHealth Northwest's use or disclosure of PHI. Customer will provide such notice no later than 15 days prior to the effective date of the change. Customer will obtain any consent or authorization that may be required by the Privacy Rule, or applicable state law, prior to furnishing CompuHealth Northwest with PHI.

4.3 Notification of Restrictions to Use or Disclosure of PHI. Customer will notify CompuHealth Northwest of any restriction to the use or disclosure of PHI that Customer has agreed to in accordance with 45 C.F.R. § 164.522 or 42 U.S.C. § 17935(a), to the extent that such restriction may affect CompuHealth Northwest's use or disclosure of PHI. Customer will provide such notice no later than 15 days prior to the effective date of the restriction. If CompuHealth Northwest reasonably believes that any restriction agreed to by Customer pursuant to this Section may materially impair CompuHealth Northwest's ability to perform its obligations under the Agreement or this BAA, the parties will mutually agree upon any necessary modification of CompuHealth Northwest's obligations under such agreements.

4.4 Permissible Requests by Customer. Customer will not request CompuHealth Northwest to use or disclose PHI in any manner that would not be permissible under the Privacy Rule, the Security Rule or the HITECH Act if done by Customer, except as permitted pursuant to the provisions of Sections 2.2, 2.3, 2.4, 2.5 and 2.6 of this BAA

#### **SECTION 5: TERM AND TERMINATION**

5.1 Term. The term of this BAA will commence as of the Effective Date, and will terminate when all of the PHI provided by Customer to CompuHealth Northwest, or created or received by CompuHealth Northwest on behalf of Customer, is destroyed or returned to Customer or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with Section 5.3.

5.2 Termination for Cause. Upon either party's knowledge of a material breach by the other party of this BAA, such party will provide written notice to the breaching party detailing the nature of the breach and providing an opportunity to cure the breach within 30 business days. Upon the expiration of such 30 day cure period, the non-breaching party may terminate this BAA and, at its election, the Agreement, if cure is not possible.

5.3 Effect of Termination.

5.3.1 Except as provided in Section 5.3.2, upon termination of the Agreement or this BAA for any reason, CompuHealth Northwest will return or destroy all PHI received from Customer, or created or received by CompuHealth Northwest on behalf of Customer, and will retain no copies of the PHI. This provision will apply to PHI that is in the possession of subcontractors or agents of CompuHealth Northwest.

5.3.2 If it is infeasible for CompuHealth Northwest to return or destroy the PHI upon termination of the Agreement or this BAA, CompuHealth Northwest will: (a) extend the protections of this BAA to such PHI; (b) limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as CompuHealth Northwest maintains such PHI; and (c) never disclose such PHI to another CompuHealth Northwest client or third party unless such information has been de-identified in accordance with the standards set forth in 45 C.F.R. § 164.514(b).

**SECTION 6: SURVIVAL**

The respective rights and obligations of CompuHealth Northwest under Section 5.3 of this BAA will survive the termination of the BAA and the Agreement.

**SECTION 7: INDEMNIFICATION**

Customer agrees to indemnify, defend and hold harmless CompuHealth Northwest and its members, managers, directors, officers, and employees from and against all losses, damages, demands, claims, suits, actions, causes of action, proceedings, assessments, judgments, awards, penalties and settlements, and all costs and expenses (including notification costs, advertising/media costs, interest, court or hearing costs and reasonable fees and expenses of attorneys and expert witnesses) of investigating, defending or asserting any of the foregoing, that are asserted against, resulting to, imposed upon or incurred by CompuHealth Northwest or any such person, directly or indirectly, by reason of or resulting from any material violation of this Agreement or any Breach by Customer or its members, managers, directors, officers, employees or agents.

**SECTION 8: EFFECT OF BAA**

In the event of any inconsistency between the provisions of this BAA and the Agreement, the provisions of the BAA will control. In the event of inconsistency between the provisions of this BAA and mandatory provisions of the Privacy Rule, the Security Rule or the HITECH Act, as amended, or their interpretation by any court or regulatory agency with authority over CompuHealth Northwest or Customer, such interpretation will control; provided, however, that if any relevant provision of the Privacy Rule, the Security Rule or the HITECH Act is amended in a manner that changes the obligations of CompuHealth Northwest or Customer that are embodied in terms of this BAA, then the parties agree to negotiate in good faith appropriate non-financial terms or amendments to this BAA to give effect to such revised obligations. Where provisions of the BAA are different from those mandated in the Privacy Rule, the Security Rule, or the HITECH Act, but are nonetheless permitted by such rules as interpreted by courts or agencies, the provisions of the BAA will control.

Customer Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print Name: \_\_\_\_\_ Title: \_\_\_\_\_

Practice or Business Name: \_\_\_\_\_

Customer Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip Code: \_\_\_\_\_

Customer Phone: \_\_\_\_\_ Customer Fax: \_\_\_\_\_

CompuHealth Northwest Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print Name: \_\_\_\_\_ Title: \_\_\_\_\_

CompuHealth Northwest Inc. 2801 Meridian Street Suite 201 Bellingham WA 98225-2400

Phone: 360-592-0926 Fax: 360-592-4595