1. Business Associate checklist
2. Business Associate Agreement
3. Business Associated with Qualified Service Organization Language Example

**HIPAA Privacy and Security 2-day Boot Camp, June 5 & 6, Helena, MT**

1. **Business Associate Agreement Checklist**

Every BAA must impose the following primary criteria on Business Associates:

1. What uses and disclosures are permitted; No other uses or disclosures unless specifically allowed;
2. Implement appropriate safeguards; Report breaches and problems;
3. Assist Covered Entity with granting individuals’ access, amendment, and accounting of disclosures;
4. Comply with other requirements applicable to Covered Entity;
5. Make available books and records to HHS;
6. At termination, return or destroy all information; Ensure that subcontractors meet the same standards;
7. Authorize termination if the Business Associate breaches the BAA.

To amend your existing BAA to include all of the new requirements of HITECH and the Omnibus Rule add the following provisions:

1. Add a definition of HITECH and the Omnibus Rule, and consider whether to include them in the definition of HIPAA.
2. Where the BAA describes the Business Associate as an entity receiving data from the Covered Entity or producing it for the Covered Entity, include the words “creates, receives, maintains or transmits.”  That is the new language defining the roles that a third-party vendor can play to become a Business Associate, and it is useful to include the same language.
3. Specifically note that the Business Associate must notify you of any “breach” as defined in HIPAA.  This can be included in the “reporting of disclosures” section or some similar location.  Remember to include a relatively short reporting period (3-5 days, usually), so that you will be able to meet your own timing requirements if the breach must be reported.  A Covered Entity has up to 60 days to report a breach, but that is an outside limit; the obligation is to report “without unreasonable delay,” and if your Business Associate delays in reporting to you, you may not be able to meet your own timing constraints.  You may be treated as knowing of the breach at the same time the Business Associate discovers it, not when they report it to you.
4. Add to the “accounting of disclosures” section a statement specifying that, if the Business Associate maintains records in electronic form, it will account for ALL disclosures for at least a 3-year period.  This is different from the original accounting requirement, which excludes many disclosures but lasts for 6 years.
5. Specifically note that the Business Associate has obligations under the HITECH Act, and require the Business Associate to acknowledge and agree to abide by those requirements.
6. Add a provision noting that the Business Associate will abide by requirements not to disclose data to insurers and other health plans if the patient pays for the service in full and requests confidentiality.  The Covered Entity will likely have to notify the Business Associate that a patient has requested such secrecy.
7. The BAA should already give the Covered Entity right to terminate if the Business Associate violates the BAA.  However, you should add a provision allowing the Business Associate to terminate the BAA if the Covered Entity fails to meet its HIPAA obligations.  This is not mentioned in the Omnibus Rule, but was specifically noted in the HITECH Act.
8. The Omnibus Rule added some language to the BAA regulations that was not otherwise mentioned in the HITECH Act.  If the Business Associate carries out one of the Covered Entity’s obligations under the Privacy Rule, the BAA must require that the Business Associate agree to abide by that Privacy Rule provision.  While this is covered conceptually in almost every BAA already, it can’t hurt to include specific language to this effect.
9. **SAMPLE BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (the “Agreement”), is entered into this \_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_\_ (the “Effective Date”), by and between (“Covered Entity”) and **[INSERT BUSINESS ASSOCIATE]** (“Business Associate”).

**PURPOSE**

The Business Associate and Covered Entity (collectively the “Parties”) are entering into this Agreement to comply with privacy standards adopted by the U.S. Department of Health and Human Services as they may be amended from time to time, 45 C.F.R. parts 160 and 164 (“the Privacy Rule”); security standards adopted by the U.S. Department of Health and Human Services as they may be amended from time to time, 45 C.F.R. parts 160, 162 and 164, subpart C (“the Security Rule”); the Health Information Technology for Economic and Clinical Health (HITECH) Act enacted as under Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 and regulations promulgated thereunder (“Omnibus Rule”); and any applicable state confidentiality laws.

**RECITALS**

WHEREAS, Business Associate provides professional services to or on behalf of Covered Entity;

WHEREAS, in connection with these services, Covered Entity discloses to Business Associate certain protected health information (“PHI”) that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”);

WHEREAS, the HIPAA Rules require that Covered Entity receive adequate assurances that Business Associate will comply with certain obligations with respect to the PHI received in the course of providing services to or on behalf of Covered Entity.

WHEREAS, HIPAA prohibits disclosure or use of PHI by Business Associate if a written contract concerning the use of PHI is not in place.

NOW THEREFORE, in consideration of the mutual promises and covenants herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

* 1. Definitions. Terms used herein, but not otherwise defined, shall have meaning ascribed by the Privacy Rule, the Security Rule, and the Omnibus Rule.
     1. Breach. “Breach is defined as disclosure not permitted by 45 C.F.R. 164.502 through 45 C.F.R. 512.
     2. Business Associate. “Business Associate” shall generally have the same meaning as the terms “business associate” at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean **[INSERT BUSINESS ASSOCIATE].**
     3. Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean **[COVERED ENTITY]**.
     4. Designated Record Set. “Designated Record Set” shall mean a group of records maintained by or for a Covered Entity that is: (i) the medical records and billing records about Individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about Individuals. For purposes of this definition, the term “record” means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
     5. HIPAA Rules. The Privacy Rule and the Security Rule and amendments codified and promulgated by the HITECH Act and Omnibus Rule are referred to collectively herein as “HIPAA Rules.”
     6. Individual. “Individual” shall mean the person who is the subject of the protected health information.
     7. Protected Health Information (“PHI”). “Protected Health Information” or PHI shall have the same meaning as the term “protected health information” in 45 C.F.R. §160.103, limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of covered entity pursuant to this Agreement.
     8. Required by Law. “Required by Law” shall mean a mandate contained in Law that compels a use or disclosure of PHI.
     9. Secretary. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his or her Designee.
     10. Security Incident. “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.
     11. Sensitive Personal Information. “Sensitive Personal Information” shall mean an individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: a) social security number; driver’s license number or government-issued identification number; or account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; or b) information that identifies an individual and relates to: the physical or mental health or condition of the individual; the provision of health care to the individual; or payment for the provision of health care to the individual.
     12. Subcontractor. “subcontractor” shall have the same meaning as the term “subcontractor” in 45 C.F.R. §160.103.
     13. Unsecured PHI. “Unsecured PHI” shall mean 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.
  2. Purposes for which PHI May Be Disclosed to Business Associate. PHI may be disclosed to and used by Business Associate only for the purposes related to the services Business Associate is performing for Covered Entity and as permitted by HIPAA Rules and any other applicable federal or state statutes, rules and regulations.
  3. Obligations and Activities of Business Associate. Business Associate agrees to comply with applicable federal and state confidentiality and security laws, specifically the provisions of the HIPAA Rules applicable to business associates, including:
     1. Use and Disclosure of PHI. Not to use or disclose protected health information other than as permitted or required by the Agreement or as required by law. Business Associate may use and disclose PHI for the proper management and administration of the business associate and to provide data aggregation services relating to the health care operations of the covered entity. Business Associate may disclose PHI for the foregoing purposes (1) if the disclosure is permitted by law, or (2)(i) if the Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person and (ii) the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.
     2. Notice to Covered Entity Prior to Disclosure. Business Associate agrees to provide written notice to Covered Entity within three days of receiving a request for PHI from law enforcement, an attorney, or court arising out of an actual or potential court proceeding, and agrees not to provide PHI prior to providing such notification.
     3. Safeguards. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement. Business Associate shall assure that all PHI be secured when accessed by Business Associate’s employees, agents, or subcontractors. Any access to PHI by Business Associate’s employees, agents or subcontractors shall be limited to legitimate business needs while working with PHI.
     4. Information Breach Notification for PHI. Report to Covered Entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required by 45 CFR 164.410, and any Security Incident of which it becomes aware. The notification of a breach by the Business Associate shall be immediately following the “discovery” (within the meaning of 45 C.F.R. §164.410(a)) of a breach of such information. Initial notification of the breach does not need to be in compliance with 45 C.F.R. §164.404(c); however, Business Associate must provide Covered Entity with all information necessary for Covered Entity to comply with 45 C.F.R. §164.404(c) without reasonable delay, and in no case later than 30 days following the discovery of the breach. Business Associate will take, or in the event that the acts or omissions of an agent or subcontractor of Business Associate gave rise to the Breach or Security Incident, will require its agent or subcontractor to take, commercially reasonable actions to mitigate any negative impact of any Breach or Security Incident and to improve safeguards to prevent recurrence. Business Associate shall be liable for the costs associated with such breach if caused by the Business Associate’s negligent or willful acts or omissions, or the negligent or willful acts or omissions of Business Associate’s agents, officers, employees or subcontractors.
     5. Disclosure to Agents and Subcontractors. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information. Business Associate shall be liable to Covered Entity for any acts, failures or omissions of the agent or subcontractor in providing the services as if they were Business Associate’s own acts, failures or omissions, to the extent permitted by law. Business Associate further expressly warrants that its agents or subcontractors will be specifically advised of, and will comply in all respects with, the terms of this Agreement.
     6. Individual Rights Regarding Designated Record Sets. If Business Associate maintains a Designated Record Set on behalf of Covered Entity Business Associate agrees as follows:
        1. Individual Right to Copy or Inspection. Business Associate agrees that if it maintains a Designated Record Set for Covered Entity that is not maintained by Covered Entity, it will permit an Individual to inspect or copy PHI about the Individual in that set as directed by Covered Entity to meet the requirements of 45 C.F.R. § 164.524. If the PHI is in electronic format, the Individual shall have a right to obtain a copy of such information in electronic format and, if the Individual chooses, to direct that an electronic copy be transmitted directly to an entity or person designated by the individual in accordance with HITECH section 13405 (c). Under the Privacy Rule, Covered Entity is required to take action on such requests as soon as possible, but not later than 30 days following receipt of the request. Business Associate agrees to make reasonable efforts to assist Covered Entity in meeting this deadline. The information shall be provided in the form or format requested if it is readily producible in such form or format; or in summary, if the Individual has agreed in advance to accept the information in summary form. A reasonable, cost-based fee for copying health information may be charged. If Covered Entity maintains the requested records, Covered Entity, rather than Business Associate shall permit access according to its policies and procedures implementing the Privacy Rule.
        2. Individual Right to Amendment. Business Associate agrees, if it maintains PHI in a Designated Record Set, to make amendments to PHI at the request and direction of Covered Entity pursuant to 45 C.F.R. §164.526. If Business Associate maintains a record in a Designated Record Set that is not also maintained by Covered Entity, Business Associate agrees that it will accommodate an Individual’s request to amend PHI only in conjunction with a determination by Covered Entity that the amendment is appropriate according to 45 C.F.R. §164.526.
        3. Accounting of Disclosures. Business Associate agrees to maintain documentation of the information required to provide an accounting of disclosures of PHI, whether PHI is paper or electronic format, in accordance with 45 C.F.R. §164.528 and HITECH Sub Title D Title VI Section 13405 (c), and to make this information available to Covered Entity upon Covered Entity’s request, in order to allow Covered Entity to respond to an Individual’s request for accounting of disclosures. Under the Privacy Rule, Covered Entity is required to take action on such requests as soon as possible but not later than 60 days following receipt of the request. Business Associate agrees to use its best efforts to assist Covered Entity in meeting this deadline but not later than 45 days following receipt of the request. Such accounting must be provided without cost to the individual or Covered Entity if it is the first accounting requested by an individual within any 12 month period; however, a reasonable, cost-based fee may be charged for subsequent accountings if Business Associate informs the individual in advance of the fee and is afforded an opportunity to withdraw or modify the request. Such accounting is limited to disclosures that were made in the six (6) years prior to the request (not including disclosures prior to the compliance date of the Privacy Rule) and shall be provided for as long as Business Associate maintains the PHI.
     7. Privacy of Individually Identifiable Health Information. To the extent the Business Associate is to carry out one or more of 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).
     8. Internal Practices, Policies and Procedures. Except as otherwise specified herein, Business Associate shall make available its internal practices, policies and procedures relating to the use and disclosure of PHI, received from or on behalf of Covered Entity to the Secretary or his or her agents for the purpose of determining Covered Entity’s compliance with the HIPAA Rules, or any other health oversight agency, or to Covered Entity. Records requested that are not protected by an applicable legal privilege will be made available in the time and manner specified by Covered Entity or the Secretary.
     9. Minimum Necessary. Business Associate shall ensure that all uses and disclosures of PHI are subject to the principle of “minimum necessary use and disclosure,” i.e., that only PHI that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request is used or disclosed; and, the use of limited data sets when possible.
     10. De-identified Information. Business Associate may use and disclose de-identified health information if written approval from the Covered Entity is obtained, and the PHI is de-identified in compliance with the HIPAA Rules. Moreover, Business Associate shall review and comply with the requirements under Section E (Permitted Uses and Disclosures) of this Agreement.
     11. Data Aggregation. In the event that Business Associate works for more than one Covered Entity, Business Associate is permitted to use and disclose PHI for data aggregation purposes, however, only in order to analyze data for permitted health care operations, and only to the extent that such use is permitted under the HIPAA Rules.
     12. Notice of Privacy Practices. Business Associate shall abide by the limitations of Covered Entity’s Notice of Privacy Practices of which it has knowledge. Any use or disclosure permitted by this Agreement may be amended by changes to Covered Entity’s Notice; provided, however, that the amended Notice shall not affect permitted uses and disclosures on which Business Associate relied prior to receiving notice of such amended Notice.
     13. Withdrawal of Authorization. If the use or disclosure of PHI in this Agreement is based upon an Individual’s specific authorization for the use or disclosure of his or her PHI, and the Individual revokes such authorization, the effective date of such authorization has expired, or such authorization is found to be defective in any manner that renders it invalid, Business Associate shall, if it has notice of such revocation, expiration, or invalidity, cease the use and disclosure of the Individual’s PHI except to the extent it has relied on such use or disclosure, or if an exception under the Privacy Rule expressly applies.
     14. Knowledge of HIPAA Rules. Business Associate agrees to review and understand the HIPAA Rules as it applies to Business Associate, and to comply with the applicable requirements of the HIPAA Rule, as well as any applicable amendments.
     15. Breach Notification to Individuals. Business Associate’s duty to notify Covered Entity of any breach does not permit Business Associate to notify those individuals whose PHI has been breached by Business Associate without the express written permission of Covered Entity to do so. Any and all notification to those individuals whose PHI has been breached shall be made under the direction, review and control of Covered Entity. The Business Associate will notify the Privacy Officer via telephone with follow-up in writing to include; name of individuals whose PHI was breached, information breached, date of breach, form of breach, etc. The cost of the notification will be paid by the Business Associate. Business Associate shall be liable for all costs associated with any breach caused by Business Associate’s negligent or willful acts or omissions, or those negligent or willful acts or omissions of Business Associate’s agents, officers, employees or subcontractors.
  4. Obligations of Covered Entity. If deemed applicable by Covered Entity, Covered Entity shall:
     1. provide Business Associate a copy of its Notice of Privacy Practices (“Notice”) produced by Covered Entity in accordance with 45 C.F.R. 164.520 as well as any changes to such Notice;
     2. provide Business Associate with any changes in, or revocation of, authorizations by Individuals relating to the use and/or disclosure of PHI, if such changes affect Business Associate’s permitted or required uses and/or disclosures;
     3. notify Business Associate of any restriction to the use and/or disclosure of PHI to which Covered Entity has agreed in accordance with 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of PHI;
     4. not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy rule if done by the Covered entity;
     5. notify Business Associate of any amendment to PHI to which Covered Entity has agreed that affects a Designated Record Set maintained by Business Associate;
     6. if Business Associate maintains a Designated Record Set, provide Business Associate with a copy of its policies and procedures related to an Individual’s right to: access PHI; request an amendment to PHI; request confidential communications of PHI; or request an accounting of disclosures of PHI; and,
     7. notify individuals of breach of their Unsecured PHI in accordance with the requirements set forth in 45 C.F.R. §164.404.
  5. Permitted Uses and Disclosures by Business Associates. Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in this Business Associates Agreement or in a Professional Services Agreement, provided that such use or disclosure would not violate the HIPAA Rules if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity. Also, Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with the HIPAA Rules.

1. Use. Business Associate will not, and will ensure that its directors, officers, employees, contractors and other agents do not, use PHI other than as permitted or required by Business Associate to perform the Services or as required by law, but in no event in any manner that would constitute a violation of privacy standards or security standards if used by Covered Entity.
2. Disclosure. Business Associate will not, and will ensure that its directors, officers, employees, contractors, and other agents do not, disclose PHI other than as permitted pursuant to this arrangement or as required by law, but in no event disclose PHI in any manner that would constitute a violation of the privacy standards or security standards if disclosed by Covered Entity.
3. Minimum Necessary. Business Associate agrees to make uses and disclosures and requests for protected health information consistent with Covered Entity’s minimum necessary policies and procedures.
4. Other Limited Uses. Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity, except for the specific uses and disclosures set forth below:
   1. Business Associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the Business Associate;
   2. Business Associate may provide data aggregation services relating to the health care operations of the covered entity.
5. Application of Security and Privacy Provisions to Business Associate.
   * 1. Security Measures. Sections 164.308, 164.310, 164.312 and 164.316 of Title 45 of the Code of Federal Regulations dealing with the administrative, physical and technical safeguards as well as policies, procedures and documentation requirements that apply to Covered Entity shall in the same manner apply to Business Associate. Any additional security requirements contained in Sub Title D of Title IV of the HITECH Act that apply to Covered Entity shall also apply to Business Associate. Pursuant to the foregoing requirements in this section, the Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the paper or electronic PHI that it creates, has access to, or transmits. Business Associate will also ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect such information. Business Associate will ensure that PHI contained in portable devices or removable media is encrypted.
     2. Annual Guidance. For the first year beginning after the date of the enactment of the HITECH Act and annually thereafter, the secretary shall annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the sections referred to in subsection (a) and the security standards in subpart C of part 164 of title 45, Code of Federal Regulations. Business Associate shall, at their own cost and effort, monitor the issuance of such guidance and comply accordingly.
     3. Privacy Provisions. The enhanced HIPAA privacy requirements including but not necessarily limited to accounting for certain PHI disclosures for treatment, restrictions on the sale of PHI, restrictions on marketing and fundraising communications, payment and health care operations contained Subtitle D of the HITECH Act that apply to the Covered entity shall equally apply to the Business Associate.
     4. Application of Civil and Criminal Penalties. If Business Associate violates any security or privacy provision specified in subparagraphs (1) and (2) above, sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d-5, 1320d-6) shall apply to Business Associate with respect to such violation in the same manner that such sections apply to Covered Entity if it violates such provisions.
6. Term and Termination.
   * 1. Term. The term of this Agreement shall be effective as of the Effective Date and shall terminate on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, or on the date Covered Entity terminates for cause as authorized in paragraph 2 of this Section, whichever is sooner.
     2. Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity if Covered Entity determines Business Associate has violated a material term of the Agreement. Covered Entity, may in its discretion provide an opportunity for Business Associate to cure the breach or end the violation within a time specified by Covered Entity, or immediately terminate the Agreement. Termination of this Agreement may at the Covered Entity’s discretion be grounds for immediate termination of any underlying services agreement. Termination of any underlying services agreement may at the Covered Entity’s discretion be grounds for immediate termination of this Agreement.
     3. Effect of Termination. Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;

Return to covered entity the remaining protected health information that the business associate still maintains in any form;

Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;

Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at Section E above under “Permitted Uses and Disclosures By Business Associate” which applied prior to termination; and

Return to covered entity the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

* + 1. Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

1. Miscellaneous.
   * 1. Indemnification. To the extent permitted by law, Business Associate agrees to defend, indemnify and hold harmless Covered Entity, its officers, employees, affiliates, subsidiaries, and agents from every claim, risk, loss, damage, demand, suit, judgment and attorney’s fee, and any other kind of expense arising from, resulting from, or in any manner directly or indirectly connected with performance of the work, functions, activities, or services provided to Covered Entity, or attributable to any acts or omissions or other conduct of Business Associate or its agents in connection with the performance of Business Associate’s or its agents’ duties under this Agreement or violations under HIPAA.

Covered Entity shall have the option, at its sole discretion, to employ attorneys selected by it to defend any such action, the costs and expenses of which shall be the responsibility of Business Associate. Covered Entity shall provide Business Associate with timely notice of the existence of such proceedings and such information, documents and other cooperation as reasonably necessary to assist Business Associate in establishing a defense to such action.

These indemnities shall survive termination of this Agreement, and Covered Entity reserves the right, at its option and expense, to participate in the defense of any suit or proceeding through counsel of its own choosing.

* + 1. Mitigation. If Business Associate violates this Agreement or either of the HIPAA Rules, Business Associate agrees to mitigate any damage caused by such breach.
    2. Rights of Proprietary Information. Covered Entity retains any and all rights to the proprietary information, confidential information, and PHI it releases to Business Associate.
    3. Notices. Any notices pertaining to this Agreement shall be given in writing and shall be deemed duly given when personally delivered to a Party or a Party's authorized representative as listed below or sent by means of a reputable overnight carrier, or sent by means of certified mail, return receipt requested, postage prepaid. A notice sent by certified mail shall be deemed given on the date of receipt or refusal of receipt. All notices shall be addressed to the appropriate Party as follows:

**If to Covered Entity:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Attn: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**If to Business Associate:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Attn: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_­

* + 1. Amendments. This Agreement may not be changed or modified in any manner except by an instrument in writing signed by a duly authorized officer of each of the Parties hereto. The Parties, however, agree to amend this Agreement from time to time as necessary, in order to allow Covered Entity’s to comply with the requirements of the HIPAA Rules.
    2. Choice of Law. This Agreement and the rights and the obligations of the Parties hereunder shall be governed by and construed under the laws of the State of Montana, without regard to applicable conflict of laws principles. Venue shall be in Montana’s Fourth Judicial District Court or in the U.S. District Court for the District of Montana.
    3. Assignment of Rights and Delegation of Duties. This Agreement is binding upon and inures to the benefit of the Parties hereto and their respective successors and permitted assigns. However, neither Party may assign any of its rights or delegate any of its obligations under this Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Notwithstanding any provisions to the contrary, however, Covered Entity retains the right to assign or delegate any of its rights or obligations hereunder to any of its wholly owned subsidiaries, affiliates or successor companies. Assignments made in violation of this provision are null and void.
    4. Nature of Agreement. Nothing in this Agreement shall be construed to create (i) a partnership, joint venture or other joint business relationship between the Parties or any of their affiliates, (ii) any fiduciary duty owed by one Party to another Party or any of its affiliates, or (iii) a relationship of employer and employee between the Parties. Neither party will have the authority to bind the other except to the extent authorized herein.
    5. No Waiver. Failure or delay on the part of either Party to exercise any right, power, privilege or remedy hereunder shall not constitute a waiver thereof. No provision of this Agreement may be waived by either Party except by a writing signed by an authorized representative of the Party making the waiver.
    6. Equitable Relief. Any disclosure of misappropriation of PHI by Business Associate in violation of this Agreement will cause Covered Entity irreparable harm, the amount of which may be difficult to ascertain. Business Associate therefore agrees that Covered Entity shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining Business Associate from any such further disclosure or breach, and for such other relief as Covered Entity shall deem appropriate. Such rights are in addition to any other remedies available to Covered Entity at law or in equity. Business Associate expressly waives the defense that a remedy in damages will be adequate, and further waives any requirement in an action for specific performance or injunction for the posting of a bond by Covered Entity.
    7. Severability. The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.
    8. No Third Party Beneficiaries. Nothing in this Agreement shall be considered or construed as conferring any right or benefit on a person not party to this Agreement nor imposing any obligations on either Party hereto to persons not a party to this Agreement.
    9. Headings. The descriptive headings of the articles, sections, subsections, exhibits and schedules of this Agreement are inserted for convenience only, do not constitute a part of this Agreement and shall not affect in any way the meaning or interpretation of this Agreement.
    10. Entire Agreement. This Agreement, together with all Exhibits, Riders and amendments, if applicable, which are fully completed and signed by authorized persons on behalf of both Parties from time to time while this Agreement is in effect, constitutes the entire Agreement between the Parties hereto with respect to the subject matter hereof and supersedes all previous written or oral understandings, agreements, negotiations, commitments, and any other writing and communication by or between the Parties with respect to the subject matter hereof. In the event of any inconsistencies between any provisions of this Agreement in any provisions of the Exhibits, Riders, or amendments, the provisions of this Agreement shall control.
    11. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Rules and any applicable state confidentiality laws. The provisions of this Agreement shall prevail over the provisions of any other agreement that exists between the Parties that may conflict with, or appear inconsistent with, any provision of this Agreement or the HIPAA Rules.
    12. Regulatory References. A citation in this Agreement to the Code of Federal Regulations shall mean the cited section as that section may be amended from time to time.

Agreed to:

**Business associate Covered entity**

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

(Authorized Signature) (Authorized Signature)

Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Type or Print) (Type or Print)

Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

**3) EXAMPLE OF HIPAA BUSINESS ASSOCATE AGREEMENT WITH QUALIFIED SERVICE ORGANIZATION AGREEMENT LANGUAGE, NOT UPDATED TO REFLECT 2017 OR 2018 42 CFR, PART 2, FINAL RULE:**

1. acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received from [insert program name] identifying or otherwise relating to the patients in the [insert program name] (‘protected information’), it is fully bound by the provision of the federal regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2; and the Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. Parts 142, 160, 162 and 164;
2. agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2, as amended;
3. agrees that it will not use or disclose protected health information except as permitted or required by the Agreement or by law;
4. agrees that, when the [insert entity name] uses, discloses, or request protected health information it will limit the use, disclosure, or request to the minimum necessary;
5. agrees that if the [insert entity name] enters into a contract with any agent, including a subcontractor, the agent will agree to comply with 42 C.F.R. Part 2 and HIPAA, and, if the [insert entity name] learns of a pattern or practice by the agent that is a material breach of the contract with the [insert entity name], to take reasonable steps to cure the breach or terminate the contract, if feasible;
6. agrees to comply with HIPAA’s security provisions with regard to electronic protected health information, and to use appropriate safe guards (*can define with more specificity*) to prevent the unauthorized use or disclosure of the protected information;
7. agrees to report breaches of protected information to the [insert program name];
8. agrees to report to the [insert program name] any use or disclosure of the protected information not provided for in this Agreement of which it becomes aware (*insert negotiated time and manner terms*);
9. agrees to ensure that any agent, including a subcontractor, to whom the Center provides protected information received from the [insert program name], or creates or receives on behalf of the [insert program name], agrees to the same restrictions and conditions that apply through this Agreement to the [insert entity name] with respect to such information;
10. agrees to provide access to the protected information at the request of the [insert program name], or to an individual as directed by the [insert program name], in order to meet the requirements of 45 C.F.R. § 164.524 which provides patients with the right to access and copy their own protected information (*insert negotiated time and manner terms*);
11. agrees to make any amendments to the protected information as directed or agreed to by the [insert program name] pursuant to 45 C.F.R. § 164.524 (*insert negotiated time and manner terms*);
12. agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure or protected information received from the [insert program name], or created or received by the [insert entity name] on behalf of the [insert program name], to the [insert program name] or to the Secretary of the Department of Health and Human Services for purposes of the Secretary determining the [insert program name]’s compliance with HIPAA (*insert negotiated time and manner terms*);
13. agrees to document disclosures of protected information, and information related to such disclosures, as would be required for the [insert program name] to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. §

164.528 (*insert negotiated time and manner terms*);

1. agrees to provide the [insert program name] or an individual in accordance with paragraph (9) of this agreement to permit the [insert program name] to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F. R. 45

C.F.R. § 164.528 (insert negotiated time and manner terms).

**Termination**

1. The [insert program name] may terminate this agreement if it determines that the [insert entity name] has violated any material term.
2. Upon termination of this Agreement for any reason, the [insert entity name] shall return or destroy all protected information received from the [insert program name], or created or received by the [insert entity name] on behalf of the [insert program name]. This provision shall apply to protected information that is in the possession of subcontractors or agents of the [insert entity name]. The [insert entity name] shall retain no copies of the protect information.
3. In the event that the [insert entity name] determines that returning or destroying the protected information is infeasible, the [insert entity name] shall notify the [insert program name] of the conditions that make return or destruction infeasible (insert negotiated time and manner terms);
4. Upon notification that the return or destruction of the protected information is infeasible, the [insert entity name] shall extend the protections of this Agreement to such protected information and limit further uses and disclosures of the information to those purposes that make the return or destruction infeasible, as long as, the [insert entity name] maintains the information.