

Business Associate Agreement

This **Business Associate Agreement** is between Consultant and Client. This Agreement provides for the terms related to the use and disclosure of PHI between Consultant and Client in accordance with the Agreement on Consulting Services. The parties agree as follows:

1. Definitions

1.1 Defined Terms. Terms defined in the preamble and the Agreement on Consulting Services have their assigned meanings and each of the following terms has the meaning assigned to it.

“**BAA**” means this Business Associate Agreement.

“**Business Associate**” has the meaning assigned to it under HIPAA, 45 CFR § 160.103, and in reference to the party to this BAA, shall mean Consultant.

“**Covered Entity**” has the meaning assigned to it under HIPAA, 45 CFR § 160.103, and in reference to the party to this BAA, shall mean Client.

“**PHI**” means protected health information, as defined under HIPAA.

1.2 Interpretive Provisions.

1.1.1 This BAA includes the interpretive provisions of the Agreement on Consulting Services.

1.1.2 A reference in this BAA to any HIPAA regulation is a reference to the HIPAA regulation in effect and as amended, as may be applicable. Any ambiguity in this BAA shall be interpreted to permit compliance with the HIPAA rules.

1.1.3 If any term of Section 6 conflicts with another term of this BAA, the term contained in Section 6 shall be controlling. Any ambiguity in Section 6 shall be resolved to permit Covered Entity to comply with the HIPAA Rules.

2. **Effective Date.** This BAA is effective on the Effective Date.

3. **Term.** The term for this BAA shall be the term defined in Section 3 of the Agreement on Consulting Services.

4. **Acknowledgement of HIPAA Duties.** The parties acknowledge that US federal regulations relating to the confidentiality of individually identifiable health information require covered entities to comply with the privacy standards adopted by the U.S. Department of Health and Human Services as they may be amended from time to time, including Subparts A and E of 45 C.F.R. §§ 160 and 164 (“**the Privacy Rule**”), the “Standards for Electronic Transactions,” Subpart A of 45 CFR §160, and Subparts A, and I – R of 45 CFR § 162 (the “Electronic Transaction Rule”), the security standards, Subpart C of 45 C.F.R. §§ 160, 162 and 164 (“**the Security Rule**”), and the “Standards for Breach Notification for Unsecured Protected Health Information,” Subpart D of 45 CFR § 164 (the “Breach Notification Rule”), adopted by the U.S. Department of Health and Human Services as they may be amended from time to time, collectively, referred to herein as “**HIPAA Rules.**” The HIPAA Rules, as well as any applicable state confidentiality laws, require Covered Entity to ensure that business associates who receive confidential

information while providing services on behalf of the Covered Entity comply with certain obligations regarding the confidentiality of health information.

5. **Purposes for which Protected Health Information May Be Used or Disclosed to Business Associate.** In connection with the Services provided by Business Associate on behalf of Covered Entity pursuant to this BAA, Covered Entity may use and disclose PHI, as defined in the HIPAA Rules, to Business Associate for the purposes of fulfilling both Covered Entity's and Business Associate's obligations under the Agreement on Consulting Services, provided that Business Associate shall not use or disclose PHI, in any manner that would constitute a violation of HIPAA Regulations if done by Covered Entity.

6. **Business Associate Obligations.** Notwithstanding any other obligations contained in this BAA, Business Associate agrees to comply with applicable federal and state confidentiality and security laws, including, but not limited to the Privacy Rule and Security Rule, including without limitation:
 - 6.1 **Use of PHI.** Business Associate shall not use or disclose PHI except as necessary to fulfil the purposes of this BAA. Business Associate is permitted to use and disclose PHI as necessary for the proper management and administration of Business Associate or to carry out its legal responsibilities and its responsibilities under this BAA. However, Business Associate shall in such case:
 - (i) provide training to members of its workforce regarding the confidentiality requirements in the HIPAA Rules and this BAA;
 - (ii) obtain reasonable assurances from the person to whom the information is disclosed that it will be held confidential and further used and disclosed only as required by law or for the purpose for which it was disclosed to the person or entity; and
 - (iv) ensure that all disclosures of PHI are subject to the principle of "minimum necessary use and disclosure," i.e., only PHI that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request may be disclosed.
 - 6.2 **Disclosure to Third Parties.** If the Business Associate discloses PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity, to agents, including a subcontractor, Business Associate shall require the agent to agree to the same restrictions and conditions that apply to Business Associate under this BAA. Business Associate shall ensure that any agent, including a subcontractor, agrees to implement reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity. Business Associate shall be liable to Covered Entity for any intentional acts, failures, or omissions of the Agent 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 will be specifically advised of the terms of this BAA.

- 6.3 Amendment. Business Associate and Covered Entity agree to take such action as is necessary to amend this Section 6 from time to time as is necessary for compliance with the requirements of the HIPAA Regulations and any other applicable law.
- 6.4 Limitation on Disclosure. Business Associate may not use or disclose PHI 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 in this BAA.
- 6.5 Notice of Privacy Practices. Business Associate shall abide by the limitations of any Notice of Privacy Practices (“Notice”) published by the Covered Entity of which it has knowledge. Covered Entity shall provide to Business Associate such Notice when it is adopted. Any use or disclosure permitted by this BAA may be amended by such Notice. However, the amended Notice shall not affect permitted uses and disclosures on which Business Associate relied prior to such notice.
- 6.6 Safeguards. Business Associate shall maintain appropriate safeguards to ensure that PHI is not used or disclosed other than as provided by this BAA or as required by law, in accordance with Subpart C of 45 CFR Part 164. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic PHI it creates, receives, maintains, or transmits on behalf of Covered Entity.
- 7. Covered Entity Obligations.**
- 7.1 Covered Entity shall notify Business Associate of any limitations in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect business associate’s use or disclosure of PHI.
- 7.2 Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect Business Associate’s use or disclosure of protected health information.
- 7.3 Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of PHI.
- 7.4 Permissible Requests. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity, except for any provision in this BAA for data aggregation, management and administration, and legal responsibilities of Business Associate.
- 8. Disclaimer of Obligations to Third Parties of Covered Entity.** Business Associate shall not be responsible for PHI safeguards in relation to any transfers of PHI made directly between the Covered Entity and a third party. It is the Covered Entity’s sole responsibility to ensure compliance of a third party with HIPAA guidelines.
- 9. Data Aggregation.** If Business Associate works for more than one Covered Entity, Business Associate is permitted to use and disclose PHI, but only to analyze data for permitted health care operations, and only to the extent that such use is permitted under the HIPAA Rules.

10. **De-identified Information.** Use and disclosure of de-identified health information is permitted, but only if:
- (i) the de-identification complies with 45 CFR §164.502(d); and
 - (ii) any such de-identified health information meets the standard and implementation specifications for de-identification under 45 CFR §164.514(a) and (b).
11. **Requests by Individuals to Business Associate.** If Business Associate receives a request from an individual to the Business Associate regarding PHI, Business Associate agrees to forward all such requests to the Covered Entity within 10 days of such request. Business Associate further agrees to assist the Covered Entity in meeting all deadlines for responding to such requests to the extent the Business Associate maintains the required information.
12. **Individual Rights Regarding Designated Record Sets.** If Business Associate maintains a designated record set (as defined in the HIPAA Rules) on behalf of Covered Entity, Business Associate agrees as follows:
- 12.1 **Withdrawal of Consent or Authorization.** If the use or disclosure of PHI in this BAA is based upon an individual's specific consent or authorization for the use of his or her PHI, and the individual revokes such consent or authorization in writing, or the effective date of such authorization has expired, or the consent or 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 any such individual's PHI except to the extent it has relied on such use or disclosure, or where an exception under the Privacy Rule expressly applies.
 - 12.2 **Correction of PHI.** Business Associate agrees that it will amend PHI maintained by Business Associate in a designated record set as requested by Covered Entity. Business Associate must incorporate amendment within 15 days of the request by the Covered Entity.
 - 12.3 **Individual Right to Copy or Inspection.** Business Associate agrees that, if it maintains PHI in a designated record set for the Covered Entity, it will permit an individual to inspect or copy PHI about the individual in that set under conditions and limitations required under 45 CFR §164.524. The Covered Entity is required to act on such requests as soon as possible but not later than 30 days following receipt of the request. Business Associate agrees to assist Covered Entity in meeting this deadline, to the extent the requested information is maintained by Business Associate and not the Covered Entity, by providing the requested information to the Covered Entity within 25 days of such request, in the form requested by Covered Entity. 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.
 - 12.4 **Individual Right to Amendment.** If Business Associate maintains PHI in a designated record set, Business Associate agrees, if it to make amendments to PHI at the request and direction of Covered Entity pursuant to 45 CFR §164.526, within 15 days of such a request. 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 right to have access to and amend PHI about the individual in a designated record set in accordance with the Privacy Rule set forth at 45 CFR §164.526, unless the regulation provides for a denial or exception that applies.

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

13. Improper Use or Disclosure.

- 13.1 Reports of Improper Use or Disclosure. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this BAA of which it becomes aware, in accordance with the Breach Notification Rule codified at 45 CFR 164.410, and any security incident of which it becomes aware.
- 13.2 Accounting of Disclosures. Business Associate agrees to make available to the individual and/or the Covered Entity from whom the PHI originated, information required for an accounting of disclosures of PHI with respect to the individual, in accordance with 45 CFR §164.528, and incorporating exceptions to such accounting designated under the regulation. Within 20 days of notice by Covered Entity to Business Associate that it has received a request for an accounting of disclosures of PHI, Business Associate shall make available to Covered Entity, or if requested by Covered Entity, to the individual, the information required to be maintained pursuant to this Paragraph 14. In the event the request for accounting is delivered directly to Business Associate, Business Associate shall within 10 days forward such request to Covered Entity. Such accounting is limited to disclosures that were made in the six (6) years prior to the request (not including any disclosures prior to the compliance date of the Privacy Rule).
- 13.2.1 Covered Entity is required to act 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.
- 13.2.2 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.
- 13.2.3 Such accounting shall be provided so long as Business Associate maintains the PHI.
- 13.3 Internal Practices, Books, and Records. Business Associate shall make available its Internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received by Business Associate on behalf of the Covered Entity to the U.S. Department of Health and Human Services or its agents for the purpose of determining compliance with the HIPAA Rules, or any other health oversight agency, or to the Covered Entity.

14. **Miscellaneous.** This BAA shall also be subject to the terms in Sections 4, 14, and 15 of the Agreement on Consulting Services.