

Sample Business Associate Agreement

This Business Associate Agreement (the “Agreement”) is entered into as of _____, 201_, (the “Effective Date”) by and between _____, (the “Covered Entity”) and _____, (the “Business Associate”), (collectively, the “Parties”).

WHEREAS, _____(Mental Health Counseling Entity or Practitioner) is a “Covered Entity” as that term is defined in the Health Insurance Portability and Accountability Act (“HIPAA”), Privacy Standards and Security Standards, 45 C.F.R. Parts 160, 164 (the “Privacy Standards” and “Security Standards”);

WHEREAS, _____(Name of Business Associate), is a “Business Associate” as that term is defined in the Privacy Standards and Security Standards, and may access, use, create, maintain, transmit, receive and/or disclose Protected Health Information (“PHI”) on behalf of the Covered Entity;

WHEREAS, pursuant to the Privacy Standards and Security Standards, the Business Associate must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and must also comply with HIPAA;

[IF APPLICABLE] WHEREAS, Covered Entity operates a drug and alcohol treatment program that must comply with the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law and regulations, 42 U.S.C. §290dd-2 and 42 C.F.R. Part 2 (“42 C.F.R. Part 2”);

[IF APPLICABLE] WHEREAS, Business Associate is also a Qualified Service Organization (“QSO”) under 42 C.F.R. Part 2 and must agree to certain mandatory provisions regarding the use and disclosure of substance abuse treatment information; and

WHEREAS, the Parties wish to enter into this Agreement to comply with the requirements of the Privacy Standards, the Security Standards, and HIPAA.

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

ARTICLE I DEFINITIONS

1.1 Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms are defined in the Privacy Standards and Security Standards (45 C.F.R. Parts 160, 164) and HIPAA.

1.2 All PHI that is created or received by the Covered Entity and disclosed or made available in any form, including paper record, oral communication, audio recording, and electronic display, by Covered Entity or its operating units to Business Associate, or is created used, accessed, maintained, transmitted, disclosed or received by Business Associate on Covered Entity’s behalf shall be subject to this Agreement.

ARTICLE II
PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

2.1 Except as limited by 45 C.F.R. 164.504(e), or as otherwise limited in this Agreement, Business Associate may use, access, create, maintain, transmit, receive or disclose PHI on behalf of, or to provide services to, Covered Entity (*check applicable provision*):

For the following specific purposes: _____

As specified in the following agreement between Business Associate and Covered Entity:

2.2 Except as otherwise limited in this Agreement, Business Associate may also use PHI as follows (check any or all that apply):

- For the proper management and administration of Business Associate
- To carry out the legal responsibilities of Business Associate
- To provide data aggregation services to Covered Entity

2.3 Business Associate may not use or disclose PHI if such use or disclosure would be a violation of the Privacy Standards or Covered Entity's Privacy Policy if done by Covered Entity.

2.4 Any use or disclosure of PHI by Business Associate must comply with the minimum necessary policies and procedures of the Covered Entity. This includes limiting the use or disclosure to a limited data set as defined by the Privacy Rule, unless the Business Associate or Covered Entity, as applicable, determines that a limited data set is not practicable.

2.5 If Business Associate and Covered Entity are also a party to any other agreement, any use or disclosure of PHI by Business Associate must be consistent with such agreement. In the event of any inconsistency between the provisions of the Agreement and the provisions of any other agreement between the parties, the terms of this Agreement shall govern.

2.6 Business Associate agrees it will not use or further disclose PHI other than as permitted or required by this Agreement or as required by law. Business Associate may not use or disclose PHI if such use or disclosure would be a violation of other applicable law.

ARTICLE III
RESPONSIBILITIES OF BUSINESS ASSOCIATE

3.1 Safeguards. Business Associate agrees to use appropriate physical, administrative or technical safeguards to prevent use or disclosure of PHI other than as permitted by this Agreement or HIPAA.

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

3.3 Reporting. Business Associate agrees to report to Covered Entity, in writing, any use, acquisition, access or disclosure of PHI in violation of the Covered Entity's HIPAA Privacy Policies of which it becomes

aware within ten (10) days of the Business Associate's discovery of such unauthorized use, acquisition, access and/or disclosure.

3.3.1 Business Associate will immediately report to Covered Entity any attempted or successful unauthorized access, use, disclosure, modification, or destruction of electronic PHI or interference with system operations in an Information System affecting such electronic PHI of which Business Associate becomes aware. If the unauthorized use, acquisition, access, or disclosure could be or is considered a Breach of Unsecured PHI, Business Associate will fully cooperate with Covered Entity to investigate, mitigate, assess any risk, resolve, and notify any Individuals, media, and HHS as determined necessary by Covered Entity. [In the event the unsecured PHI includes any of the following: a Massachusetts resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account, then Business Associate shall notify Covered Entity of that fact and cooperate with Covered Entity for the purpose of reporting the breach under Massachusetts law to affected individuals, the Massachusetts Attorney General, and the Office of Consumer Affairs and Business Regulation.] Covered Entity will have sole discretion in addressing and responding to any purported Breach.

3.3.2 To the extent that the Breach is the result of action or inaction on the part of Business Associate, Business Associate shall be obligated to reimburse, indemnify and hold Covered Entity harmless for any costs or expenses, including attorney's fees and expenses, related to the Breach investigation, assessment, notification and resolution.

3.4 Subcontractors. In the event that Business Associate is permitted by law to provide PHI to an agent, Business Associate agrees to ensure that its agents, including a subcontractor, to whom it provides PHI received from, maintained, used, disclosed, accessed, created or received by Business Associate on behalf of Covered Entity, agrees, in writing, to the same restrictions and conditions that apply to Business Associate with respect to such information.

3.5 Right of Access. Business Associate agrees to make PHI available to the Covered Entity or to an individual as directed by the Covered Entity in accordance with the access of individuals to PHI provisions of the Privacy Standards as set forth in 45 C.F.R. §164.524 within ten (10) days of Covered Entity's request. Additionally, if the Business Associate maintains PHI in an electronic health record, it shall provide a copy of such record in an electronic format upon request.

3.6 Right of Amendment. Business Associate agrees to make PHI available for amendment and to incorporate any amendments to PHI as directed or agreed to by the Covered Entity in accordance with the amendment of PHI provisions of the Privacy Standards as set forth in 45 C.F.R. §164.526 within ten (10) days of Covered Entity's request.

3.7 Right to Accounting of Disclosures. Business Associate agrees to make an accounting of disclosures of PHI in the format provided by Covered Entity to Business Associate within ten (10) days following the request of Covered Entity. Business Associate shall make this information available to Covered Entity, or to an individual if directed by Covered Entity, or to an individual directly if requested by the individual (with notice to Covered Entity), as necessary for the Covered Entity to provide an accounting of disclosures in accordance with 45 C.F.R. §164.528.

3.8 Requests. In the event that Business Associate receives a request from an Individual or patient for Access, Amendment or Accounting purposes as described in Sections 3.5 – 3.7 above, Business Associate will immediately notify Covered Entity in writing of said request and provide reasonable assistance to Covered Entity in responding to said request in a timely fashion so as to permit Covered Entity to respond to the request within the time limits imposed under the HIPAA Standards and in any event, no later than ten (10) days following the request. Covered Entity will have sole and exclusive authority in overseeing the response to an Individual's or patient's request and Business Associate will not provide any response to an Individual or patient without first notifying Covered Entity in writing and complying with the reasonable instructions from Covered Entity.

3.9 Books and Records. Business Associate agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to Covered Entity and/or the Department of Health and Human Services in a time and manner that are mutually agreeable to the Parties and to the Secretary for purposes of determining the Covered Entity's compliance with the Privacy Standards.

3.10 Security Provisions. Business Associate will take the following measures:

- a) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that it creates, receives, maintains, accesses, uses, discloses or transmits on behalf of the Covered Entity as required by the Security Rule in accordance with 45 CFR 164.308, 164.310, 164.312 and 164.316;
- b) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to enter into a written agreement that implements the requirements imposed on Business Associate under this Agreement to protect the electronic PHI;
- c) Develop and enforce appropriate policies, procedures and documentation standards, including designation of a security official; and
- d) Report to the Covered Entity any security incident (as defined in 45 CFR 164.304) of which it becomes aware.

3.11 Judicial Proceedings. In the event that Business Associate receives a request from a third party for PHI, Business Associate will immediately notify Covered Entity in writing of said request and provide reasonable assistance to Covered Entity in responding to said request in a timely fashion so as to permit Covered Entity to respond to the request within the time limits imposed under the HIPAA Standards. Business Associate will withhold access to PHI that is subject to a subpoena, pending the resolution of judicial proceedings by the Covered Entity to resist efforts to obtain access to PHI and will resist in judicial proceedings any efforts to obtain access to PHI unless access is expressly authorized by the client, court order or other legal mandate.

ARTICLE IV RESPONSIBILITIES OF QUALIFIED SERVICE ORGANIZATION

To the extent that Business Associate is also considered a Qualified Service Organization ("QSO"), with access to protected substance abuse treatment information, Business Associate agrees to the following:

4.1. In receiving, storing, processing or otherwise dealing with any protected substance abuse information from Covered Entity, Business Associate is fully bound by the provisions of the federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2.

4.2. If necessary, Business Associate will resist in judicial proceedings any efforts to obtain access to protected substance abuse information unless access is expressly permitted under 42 C.F.R. Part 2.

4.3. Business Associate acknowledges that any unauthorized disclosure of information under this section is a federal criminal offense.

ARTICLE V TERM AND TERMINATION

5.1 Term. This Agreement shall become effective on the Effective Date and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created, maintained, accessed, transmitted, disclosed, used 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, protections are extended to such information, in accordance with the termination provisions in Section 5.2 and 5.3.

5.2 Termination. If either party fails to perform any material obligation pursuant to this Agreement, and (i) cure of the failure to perform the material obligation is possible and the failure to cure continues for a period of ten (10) days after the breaching party is notified in writing by the non-breaching party of said failure to perform, or; (ii) cure is not possible, then the non-breaching party may terminate the Agreement immediately by written notice of same to the breaching party. Covered Entity, if the non-breaching party, may also terminate any other agreement between the parties that involves the use or disclosure of PHI, in the event that Business Associate fails to perform any material obligation pursuant to this Agreement. In addition, Covered Entity may terminate this Agreement without cause upon thirty (30) days written notice to Business Associate.

5.3 Effect of Termination. Upon termination of this Agreement, for any reason, Business Associate or Covered Entity shall, as directed by Covered Entity or Business Associate, return or destroy all PHI received from, or created, maintained, used, disclosed, transmitted or received by Business Associate or Covered Entity, on behalf of either Party that either Party still maintains in any form and retain no copies of such information. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate and Business Associate shall take all necessary action to ensure that each subcontractor complies with these provisions upon termination. If return or destruction is not feasible, Business Associate or Covered Entity shall provide to the other Party notification of the conditions that make return or destruction infeasible. If Covered Entity or Business Associate is in agreement that return or destruction is not feasible, then Covered Entity or Business Associate will agree to extend the protections of this Agreement to the information and to limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible, for as long as Business Associate or Covered Entity maintains such PHI. The obligations under this section shall survive termination of this Agreement.

ARTICLE VI MISCELLANEOUS

6.1 Indemnification. Business Associate shall indemnify and hold Covered Entity harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards or other expenses, of any kind or nature whatsoever, including, without limitation, attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any breach or alleged breach of this Agreement by Business Associate.

6.2 Regulatory Reference. A reference in this Agreement to a section in the Privacy Standards, Security Standards, HIPAA or 42 C.F.R. Part 2 means the section as in effect or as amended.

6.3 Preemption. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the Privacy Standards, Security Standards, HIPAA or 42 C.F.R. Part 2, as amended, the Privacy

Standards, Security Standards, HIPAA and 42 C.F.R. Part 2 shall control. In the event of an inconsistency between the provisions of the Privacy Standards, Security Standards, HIPAA, 42 C.F.R. Part 2 and other applicable confidentiality laws, the provisions of the more restrictive rule will control.

6.4 Independent Entities. None of the provisions of this Agreement is intended to create, nor shall any be construed to create, any relationship between the Parties other than that of independent entities contracting with each other solely to effectuate the provisions of the Agreement.

6.5 Severability. The invalidity or unenforceability of any term or provision of this Agreement shall not affect the validity or enforceability of any other term or provision.

6.6 Amendments. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Standards, Security Standards, HIPAA, 42 C.F.R. Part 2 and any future regulations, statutes or other guidance concerning HIPAA or 42 C.F.R. Part 2 that may affect this Agreement.

6.7 No Third-Party Beneficiaries. This Agreement shall not in any manner whatsoever confer any rights upon or increase the rights of any third-party.

6.8 Survival of Terms. The obligations of Business Associate under Article II, III, IV, and V of this Agreement shall survive the expiration, termination, or cancellation of this Agreement and shall continue to bind Business Associate, its agents, employees, subcontractors, successors, and assigns as set forth herein.

6.9 Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Standards, Security Standards, HIPAA, 42 C.F.R. Part 2, and state social worker licensing laws.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year written below.

MENTAL HEALTH COUNSELOR/COVERED ENTITY:

BUSINESS ASSOCIATE:

By: _____

By: _____

Title: _____

Title: _____

Date: _____

Date: _____