[INSERT NAME OF MENTAL HEALTH COUNSELING ORGANIZATION]

Policy Number: _____	**Effective Date: __/__/____**
Subject: _____	**Revised: __/__/__**
Policy Name: Business Associates	**Approved:_____**

POLICY

Prior to any Protected Health Information (PHI) being shared with a Business Associate, there must be a written agreement between the Covered Entity and the Business Associate under which the Business Associate must appropriately safeguard the PHI and comply with the Privacy and Security Standards and the Covered Entity's Privacy Policies. A Business Associate must comply with the Privacy and Security Standards and the Covered Entity's Privacy Policies to the same extent, and is subject to the same penalties, as a Covered Entity.

DEFINITION

1. A Business Associate is a person or entity, other than a member of the workforce of the Covered Entity, who:

    1.1 Performs functions or activities on behalf of, or provides certain services to, a Covered Entity that involve access by the Business Associate to PHI, including the creation, reception, transmission or maintenance of PHI.

2. Examples of functions involving the use or disclosure of PHI:

    2.1 Claims processing or administration
    2.2 Data analysis
    2.3 Data processing or administration
    2.4 Utilization review
    2.5 Quality assurance
    2.6 Patient safety activities
    2.7 Billing
    2.8 Benefit management
    2.9 Practice management
    2.10 Repricing

3. Examples of services where a person or organization may need access to PHI:

    3.1 Legal services
    3.2 Actuarial services
    3.3 Accounting services
    3.4 Consulting services
    3.5 Data aggregation services
    3.6 Management services

3.7 Administrative services
3.8 Accreditation services
3.9 Financial services

4. Persons or organizations providing these services are Business Associates only if they need more than just an incidental access to PHI in order to perform the services or if they maintain PHI on behalf of a Covered Entity and have the persistent opportunity to access such PHI.

5. An individual person may be a Business Associate. However, an employee or other member of the workforce of the Covered Entity is not a Business Associate.

6. A Covered Entity may be a Business Associate of another Covered Entity if it performs Business Associate services for that covered entity.

7. A subcontractor that creates, receives, maintains or transmits PHI on behalf of another Business Associate is a Business Associate of each Business Associate.

AGREEMENT

1. Requirement of Agreement. PHI may not be shared with a Business Associate after the compliance date unless there is a written agreement that complies with this policy. This applies to any entity, including entities that have provided services to the Covered Entity before the compliance date. The compliance date for Business Associate agreements is as follows:

Date of New Agreement, Renewal of Agreement or Modification of Agreement	**Compliance Date**
Agreement in place before January 25, 2013 and not renewed or modified between March 26, 2013 and September 23, 2013	September 22, 2014
Agreement renewed or modified between March 26, 2013 and September 23, 2013	September 23, 2013

Note: Business Associate agreements that automatically renew ("Evergreen" agreements) are still eligible for the extended compliance deadline of September 22, 2014.

2. An agreement is not required if the Business Associate is a health care provider performing functions or providing services for purposes of treating a patient/client.

3. Elements of Agreement. The agreement must contain the following provisions:

3.1 A statement that the Business Associate must comply with all of the requirements imposed under HIPAA;

3.2 A description of how the Business Associate may use PHI disclosed to it, a requirement that the Business Associate use appropriate safeguards to prevent any other uses, and a

requirement that the Business Associate mitigate any harmful effect known to it of a use or disclosure that violates the agreement;

3.3 A prohibition on any use or disclosure of PHI which violates the Privacy and Security Standards or the Covered Entity's Privacy Policies;

3.4 A statement that the Business Associate, in using or disclosing PHI, comply with the minimum necessary policies and procedures of the Covered Entity, which includes limiting the use or disclosure to a limited data set as defined in the Privacy Rule, unless the Business Associate and/or Covered Entity determines that a limited data set is not practicable;

3.5 A statement that the Business Associate must report to the Covered Entity any use or disclosure of PHI not permitted under the agreement, and must also comply with the Breach Notification requirements under HIPAA [and under Massachusetts state law, if applicable] for a breach of unsecured PHI (which is PHI that is not encrypted, or otherwise shredded or physically destroyed) or personal information of a Massachusetts resident [for purposes of this policy, "personal information" includes: 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];

3.6 A requirement that any subcontractors of the Business Associate that create, receive, maintain or transmit PHI on behalf of the Business Associate agree in writing to the same restrictions, conditions and requirements that apply to the Business Associate with respect to such information and sign an Business Associate agreement with the Business Associate to that effect;

3.7 A statement that the Business Associate, and not the Covered Entity, is liable for any breaches of PHI by the Business Associate's subcontractor.

3.8 A statement that the Business Associate must cooperate in honoring patients'/clients' rights to access PHI, to request amendments, and to receive an accounting of disclosures of PHI;

3.9 A requirement that the Business Associate make its records available for audit by the Secretary of Health and Human Services for monitoring compliance with the Privacy and Security Standards and the Covered Entity's Privacy Policies, and shall also make its records available to the Covered Entity;

3.10 A statement that the Business Associate shall comply with the Security Rule, including ensuring the confidentiality, integrity and availability of electronic PHI, implementing safeguards, ensuring that agents and subcontractors do the same, developing and enforcing appropriate policies and procedures, and reporting security incidents to the Covered Entity;

3.11 A requirement that any subcontractors of the Business Associate that create, receive, maintain or transmit PHI on behalf of the Business Associate agree in writing to the same restrictions, conditions and requirements that apply to the Business Associate with respect to such information and sign a Business Associate agreement with the Business Associate to that effect;

3.12 A requirement that, on termination of the agreement, the Business Associate return or destroy all PHI (or if that is not feasible, continue to protect the confidentiality of PHI);

3.13 A provision that allows the Covered Entity to terminate the agreement if the Business Associate has violated a material term of the agreement (other than a required termination as further described below).

4. The agreement may also permit the Business Associate to use information it receives for the proper management of its business, to carry out its legal responsibilities, or for data aggregation purposes.

5. Required Termination of Agreement. If the Covered Entity or the Business Associate comes to know of a pattern of activity or practice of the other party that violates its obligations under the agreement, and the Business Associate or Covered Entity does not halt this activity or practice, then the Covered Entity or Business Associate must either terminate the agreement or report the problem to the Secretary of Health and Human Services.

ATTACHMENT

Sample Business Associate Agreement

REFERENCES

45 C.F.R. § 160.103
45 C.F.R. § 164.104
45 C.F.R. § 164.306
45 C.F.R. § 164.410
45 C.F.R. § 164.500
45 C.F.R. § 164.502(e)
45 C.F.R. § 164.504(e)
45 C.F.R. § 164.532(d)
M.G.L. c. 93H