CHAPTER 7

BUSINESS ASSOCIATES

I. GENERAL RULE

DMH may disclose Protected Health Information (PHI) to a Business Associate or allow it to create or receive PHI on DMH's behalf only if DMH obtains satisfactory assurances from the Business Associate with regard to three items listed below:

1. The Business Associate will limit its use and disclosure of PHI that it receives or creates to the purposes for which it was engaged by DMH.

2. The Business Associate will safeguard the PHI that it receives or creates from misuse in compliance with state and federal privacy laws and regulations.

3. The Business Associate will assist DMH in meeting its responsibilities to provide individuals with access to their PHI and Audit Trails of disclosures in accordance with DMH policies and procedures.

DMH must document the assurances either in a written contract or in another similar written agreement with the Business Associate. This written contract or agreement does not have to be a stand-alone document; it can be part of a broader contract or agreement (e.g., the service contract).

DMH shall disclose PHI to a Business Associate only for the purpose of assisting DMH in fulfilling its statutory obligations and not for independent use by the Business Associate.

The Business Associate requirements do not apply to disclosures made by DMH to a Health Care Provider for treatment purposes only.

II. SPECIFIC REQUIREMENTS

A. Definition of Business Associate

A Business Associate is a person or entity, other than a DMH Workforce Member, who, on behalf of DMH, performs or assists in the performance of (1) a function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, utilization

review, quality assurance, billing, benefits management, practice management and re-pricing; or (2) any other function or activity regulated by HIPAA; or (3) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services.

The following are examples of Business Associate relationships: Joint Commission for Accreditation of Healthcare Organizations (JCAHO) for purposes of accrediting a DMH facility; a vendor providing residential services to DMH clients; a vendor processing claims information for a DMH facility or Area; and a contracted hearing officer.

NOTE: DMH may be a Business Associate for another Covered Entity if it performs services on behalf of that Covered Entity (e.g., when a Covered Entity purchases services from DMH.). (See Section III.F.) However, although many of DMH's service vendors are Covered Entities, DMH in most instances is not their Business Associate, because DMH does not perform a function, activity or service on their behalf.

B. Required Terms and Conditions of a Business Associate Contract or Agreement

The written agreement between DMH and a Business Associate must meet the following requirements as are applicable:

1. **Establish the permitted and required uses/disclosures of PHI by the Business Associate.**

2. **Limit the independent use of PHI by the Business Associate**. The agreement may not authorize the Business Associate to use or disclose PHI received from or on behalf of DMH for its own purpose except as follows:

   a. It may permit the Business Associate to use the PHI if necessary for the proper management and administration of the Business Associate or to carry out its legal responsibilities.

   b. It may permit the Business Associate to disclose PHI if the disclosure is Required by Law or if the Business Associate obtains reasonable assurances that the confidentiality of the PHI will be maintained.

   Notwithstanding Subsections II.B 1 and 2, the Business Associate cannot use or disclose PHI if the use or disclosure would violate HIPAA if done by DMH or if the use or disclosure would conflict with a statement made in the Department's Notice of Privacy Practices.

3. **Include the following Business Associate Responsibilities.** The agreement must provide that the Business Associate will:

   a. not use or disclose PHI, except as authorized under the agreement or as required by law.

   b. use appropriate safeguards to prevent unauthorized use or disclosure of PHI.

   c. report to DMH immediately any unauthorized use or disclosure of which it becomes aware.

   d. report to DMH immediately any instance where PHI is requested, subpoenaed, or becomes the subject of a court order, administrative order or other legal process. Note: a subpoena is not sufficient, in and of itself, for the release of PHI.

   e. ensure that any agents or subcontractors to whom it provides such PHI agree to the same restrictions and conditions that apply to it under the agreement.

   f. make PHI available for access by the individual or his/her Personal Representative in accordance with DMH policy and procedures and/or provide DMH with such PHI in a timely fashion to allow DMH to provide such access. (See Section III.D.)

   g. accept and process requests from individuals for amendment, and incorporate approved amendments, statements of disagreements, rebuttals, etc., in the PHI, and/or or make PHI available to DMH to process and incorporate documents related to such requests, in accordance with DMH policy and procedures. (See Section III.D.)

   h. maintain or make information available, to individuals and/or DMH, for the provision of an Audit Trail of disclosures in accordance with DMH policy and procedures. (See Section III.D.)

   i. make its internal practices, books and records relating to its receipt or creation of PHI on behalf of DMH available to DMH and/or the Office of the U.S. Secretary of Health and Human Services for purposes of determining its compliance with the agreement and federal requirements.

   j. if feasible, give to DMH, or destroy, all PHI upon termination of the agreement; or, if PHI is retained, continue to extend to the PHI

the full protections specified in the agreement for so long as the PHI is maintained.

4. **Termination**. The agreement must authorize termination of the agreement by DMH upon material breach by the Business Associate of the terms of the agreement relating to use/disclosure and/or safeguarding of PHI. This element of the agreement may be omitted if the Business Associate is another governmental entity and the termination would be inconsistent with the statutory obligations of the entity.

C. Required Terms of a Business Associate Contract or Agreement if the Business Associate is Another Governmental Entity

The written agreement does not need to contain specific provisions as required under Sections II.B.2. and 3, if other law or regulations contain requirements applicable to the Business Associate that accomplish the same objective.

D. DMH Oversight and Other Responsibilities Regarding Business Associates

DMH responsibilities in Business Associate relationships include the following:

1. Applying the Minimum Necessary Rule to all disclosures to a Business Associate. (See Chapter 9, Minimum Necessary Rule.) This means that DMH Workforce Members must make all reasonable efforts not to use or disclose more than the minimum amount of PHI necessary to accomplish the intended proposes of the disclosure or use.

2. Providing the Business Associate with the necessary information and documentation to assure that the Business Associate complies with DMH privacy policies and procedures.

3. If DMH becomes aware of a material breach of the Business Associate agreement by the Business Associate, it must take action to cure the breach or to otherwise end the violation, and, if the attempt to cure or end the violation is unsuccessful, it must terminate the agreement. If termination is not feasible, DMH must report the problem to the U.S. Secretary of Health and Human Services.

4. Receiving, logging and following-up complaints regarding the use and disclosure of PHI by Business Associates.

E. Functions or Activities Required By Law

If a Business Associate is required by law to perform a function or activity on behalf of DMH, or to provide a service to DMH (e.g., the Attorney General's Office), DMH may disclose PHI to the Business Associate to the extent necessary to enable compliance with the legal requirement, without a written contract or agreement, if:

1. DMH attempts in good faith to obtain satisfactory assurances from the Business Associate that the Business Associate will protect PHI to the extent specified in Section II.B.2 and 3; and

2. If such attempt fails, DMH documents the attempt and the reasons that such assurances cannot be obtained.

III. DMH PROCEDURES FOR IDENTIFYING AND MANAGING BUSINESS ASSOCIATES

A. Boilerplate Business Associate Language

1. Development. DMH shall develop and update as necessary Business Associate language (Meeting the requirements of Section II.B.) that will be included in every contract, Interdepartmental Service Agreement (ISA) and Memorandum of Understanding (MOU) between DMH and a Business Associate. Similarly, DMH will develop appropriate language to be included in all Requests for Response (RFR) and Requests for Proposal (RFP) that could result in a Business Associate relationship. It also shall develop guidelines for those portions of the boilerplate that will require language to be inserted to individualize the relevant document. The DMH Privacy Officer shall approve all boilerplate language and guidelines.

2. Implementation. The DMH Division or Area that issues a RFR or RFP that has been identified as one that could result in a Business Associate relationship (Section III.B.) and/or who enters into a contract, ISA or MOU with an individual or entity that has been identified as a DMH Business Associate (Section III.B.), must include in the applicable RFR, RFP, contract, ISA or MOU the Business Associate boilerplate language that has been approved by the DMH Privacy Officer. No changes or modifications shall be made to the boilerplate language unless approved by the DMH Privacy Officer, or designee, in consultation with the Legal Office.

B. Identifying DMH Business Associates

1. **RFRs and RFPs issued on or after April 14, 2003.** Prior to issuing a RFR or RFP to procure a good or service, the DMH Division or Area responsible for the RFR or RFP shall submit to the DMH Privacy Officer a written analysis concerning whether or not the winning vendor(s) will be a Business Associate of DMH. The DMH Privacy Officer, in consultation with the Legal Office, shall make the final determination of any potential vendor's status as a Business Associate and shall notify the Central Office Division or Area and the Central Office Contracts Unit of such determination in writing. If the DMH Privacy Officer determines that any potential vendor will be a Business Associate, the Business Associate language must be included in the RFR or RFP. (See Section III.A.)

2. **Contracts, ISAs and MOUs executed on or after April 14, 2003.** Unless the RFR and RFP process outlined above in Section III.B.1., was followed, a Central Office Division, or Area, prior to executing a contract, ISA or MOU on or after April 14, 2003, must submit to the DMH Privacy Officer a written analysis as to whether or not the other contracting entity or person will be a Business Associate of DMH. The DMH Privacy Officer, in consultation with the Legal Office, shall make the final determination and notify the Division or Area and the Central Office Contracts Unit of its decision in writing. If the DMH Privacy Officer determines that the contract, ISA or MOU will result in the other entity or person being a DMH Business Associate, then the Business Associate language must be included in the applicable contract, ISA or MOU. (See Section III.A.)

3. **Contracts, ISA and MOUs executed prior to April 14, 2003**. The DMH Privacy Officer, working with the Legal Office, the Mental Health Services Division, and the Central Office Contracts and Accounting Units will review all contracts, ISAs and MOUs that were executed prior to April 14, 2003, and that are expected to continue in existence after April 14, 2003, to determine which, if any, create DMH Business Associates. A list of such contracts, ISAs and MOUs will be developed and circulated to all relevant DMH Divisions and Areas. The DMH Division or Area responsible for the contracts, ISAs and/or MOUs that are so identified, must add Business Associate boilerplate language to such documents. The language must be added when the contract, ISA or MOU is first amended or renewed after April 14, 2003, but in all events prior to April 14, 2004. However, pursuant to the transitional rules under HIPAA, if a contract, ISA or MOU was executed on or after October 15, 2002, or if a contract, ISA or MOU substantially was amended after October 15, 2002 (resulting in a change in program scope), the contract, ISA or MOU must be

amended to include Business Associate language by April 14, 2003 or as soon thereafter as is feasible.

4. **Documentation.** The DMH Central Office Contracts Unit shall keep an updated list of all DMH Business Associates that result from contracts and the DMH Central Office Accounting Unit shall keep a list of all DMH Business Associates resulting from ISAs and MOUs.

C. Monitoring Business Associates

1. General. The Central Office Division or Area Workforce Member(s) responsible for monitoring performance under the contract, ISA and MOU with a DMH Business Associate also shall be responsible for monitoring compliance with Business Associate terms of that contract, ISA and MOU. The DMH Privacy Officer shall be available to assist such Workforce Members as is necessary and shall develop and help implement monitoring guidelines.

2. **Breach by a Business Associate.** If the Central Office or Area DMH Workforce Member responsible for a contract, ISA, or MOU with a Business Associate becomes aware of a practice or pattern of the Business Associate that constitutes a material breach or violation of the Business Associate terms as set forth in the contract, ISA or MOU, the Workforce Member must notify the DMH Privacy Officer. Efforts to cure the breach or end the violation must be coordinated with the DMH Privacy Officer. If efforts to cure the breach or violation fail, as determined by the DMH Privacy Officer in consultation with the Legal Office, the contract, ISA or MOU must be terminated if feasible, and, if not feasible, reported in accordance with Section II.D.

D. Assess to Records and Audit Trail Information

Business Associate records that meet the definition for Designated Record Set (DRS) and are created or maintained for services rendered by or on behalf of DMH are DMH DRS(s). Such records are subject to access and amendment by the individual who is the subject of the PHI and/or his/her Personal Representative, if any. If the Business Associate also is a Covered Entity, the Business Associate will be responsible for providing access and for appropriately amending the PHI contained in any DRS that it maintains. If the Business Associate is not a Covered Entity, DMH will be responsible for processing requests for amendment and for access.

E. Complaints Regarding a DMH Business Associate's Use/Disclosure/Maintenance of PHI and/or Policies Regarding PHI

If a DMH Work Force Member receives a complaint or a report from any source about inappropriate use or disclosure of PHI by a Business Associate, the Workforce Member will report such information to the DMH Privacy Officer and the applicable Area or Central Office Contract Office. The DMH Privacy Officer will document the report or complaint in the Privacy Complaint Log (See Chapter16, Privacy Complaint Process) and the Contracts Office must document the report or complaint in the applicable contract, ISA or MOU file.

The DMH Privacy Officer, in coordination with the DMH Workforce Member responsible for monitoring performance under the contract, ISA or MOU, will take the following steps, as appropriate:

1. Request the Business Associate to review the circumstances related to the applicable complaint and to file a written response.

2. Develop a corrective action plan with the Business Associate that includes how the effects of the inappropriate use or disclosure will be mitigated.

3. Terminate the contract, ISA, or MOU if compliance cannot be obtained and termination is feasible, or report the problem to the U.S. Secretary of Health and Human Services in accordance with Section II.B.

4. Log the findings and action taken in the Privacy Complaint log and the applicable contract, ISA or MOU.

F. When DMH is identified as a Business Associate

If an entity (or person) determines that DMH is its Business Associate, then the DMH Privacy Officer, in consultation with the Legal Office, must review and approve the Business Associate terms that are part of any agreement that the entity (or person) wants DMH to sign.

IV. LEGAL REFERENCE

HIPAA 45 CFR 160.103
45 CFR 164.502(e)
45 CFR 164.504(e)