CHAPTER 1

ADMINISTRATIVE REQUIREMENTS

I. GENERAL RULE

DMH must establish and maintain appropriate administrative safeguards to prevent any intentional or unintentional violation of state or federal privacy laws.

II. SPECIFIC REQUIREMENTS AND DMH PROCEDURES

A. Personnel Designation

DMH must designate and document the designation of the following individuals:

1. **Privacy Officer.** A Privacy Officer who is responsible for the development, implementation, and maintenance of and adherence to department-wide policies and procedures related to safeguarding Protected Health Information (PHI). (See Handbook Appendix D.) The Privacy Officer must work closely with others in DMH to assure compliance with all federal and state laws and regulations and DMH policies and procedures related to PHI.

2. **Contact Person.** A contact person or office responsible for receiving complaints relating to PHI and for providing information about DMH's privacy policies and procedures. The contact person and the Privacy Officer may be the same individual. (See Appendix D.)

B. Training Requirements

DMH must take the following training actions:

1. Upon the issuance of the Privacy Handbook, all DMH Workforce Members must receive training on applicable DMH policies and procedures relating to PHI as is necessary and appropriate for such persons to carry out their job functions within DMH.

2. Each DMH Workforce Member who begins working after April 14, 2003 shall receive the training as described above within a reasonable time after joining the DMH Workforce.

3. Each DMH Workforce Member, whose functions are impacted by a material change in the policies and procedures relating to PHI, or by a

change in his/her position or job description, must receive the training as described above within a reasonable time after the change becomes effective.

4. The contents of each training developed and implemented pursuant to this Section II.B must be documented and retained by the DMH Privacy Officer. The documentation shall be retained for thirty (30) years from the last date of the applicable training using the contents, or if a shorter period of time, when the training no longer appears in the training record of a current DMH Workforce Member.

5. Training participation must be recorded in the manner prescribed by the DMH Privacy Officer for a particular training (e.g., attendance sign-in, satisfactory completion of examination, etc.) and the applicable Staff Development Office shall keep a record of all privacy trainings attended by a DMH Workforce Member. At a minimum such documentation shall be retained for six years from the date such individual ceases to be a DMH Workforce Member.

C. Policies and Procedures

1. **Required Policies and Procedures and Documentation.** DMH shall design and implement policies and procedures to assure the appropriate protection of PHI by DMH Workforce Members and Business Associates. Copies of each DMH policy and procedure relating to PHI that is implemented by DMH shall be retained by the DMH Privacy Officer for a minimum of six (6) years from the date the policy or procedure was last in effect.

2. **Changes.** DMH's policies and procedures relating to PHI must be changed as necessary to conform to changes in federal or state laws and regulations. Additionally, such policies and procedures shall be reviewed periodically to ensure that they continue to be appropriate, taking into account changes within DMH and any complaints and suggestions that have been received relating to the use or disclosure of PHI. DMH may not implement a change to a policy or procedure unless a corresponding change is made to the DMH Notice of Privacy Practices. (See Chapter 4, Notice of Privacy Practices.)

D. Complaint Process

DMH must have in place a process for individuals to make complaints about DMH's policies and procedures relating to PHI and/or DMH's compliance with those policies and procedures. DMH must document all complaints received and the disposition of each complaint. (See Chapter 16, Privacy Complaint Process.)

E. Reports of Non-Compliance and/or Recommendations for Change to Privacy Policies Made by DMH Workforce Members

The following procedures will be followed for reviewing reports of breaches of, or recommendations for, changes in DMH policies or procedures pertaining to PHI made by DMH Workforce Members.

1. **DMH Privacy Officer.** In addition to reviewing potential breaches of privacy reported through the complaint process (see Chapter 16, Privacy Complaint Process), the DMH Privacy Officer, or designee, shall review and, when appropriate, investigate any breach of privacy that is reported by DMH Workforce Members and/or Business Associates.

2. **Log.** The DMH Privacy Officer shall maintain a log of such reports. At a minimum, the log shall include the date that the report was received, the DMH location and/or Business Associate affected by the report, the PHI involved, the applicable DMH policies and/or procedures, and the action taken in response. The log shall be maintained so that information about reports or non-compliance filed in the immediate preceding six (6) years is readily retrievable.

3. **Fact-Finding.** If fact-finding is needed, the fact-finding process outlined in Section III.C.5. of Chapter 16, Privacy Complaint Process, shall be used.

4. **Report Outcomes.**

    a. **Unsubstantiated Violation of Privacy Policy and Procedures.** If the DMH Privacy Officer, or designee, determines that a violation did not occur and/or that applicable DMH policies and procedures are in compliance with state and federal law, a written notice of this shall be provided to the DMH Workforce Member who made the report. No further action is required.

    b. **Violation of Privacy Policy and Procedures Confirmed.** If the Privacy Officer, or designee, confirms that a violation of privacy policies and procedures occurred, steps shall be taken to contain any potential harm to the subject of the PHI (Mitigation, Section II.F.) and to assure that there are no future unauthorized uses or disclosures of PHI. In determining the corrective action to be taken, the following are to be considered:

        i. the need for additional training;
        ii. Workforce Member discipline; and

iii. changes to policies or procedures.

5. **DMH Workforce Members' Recommendations for Changes in Privacy Policies.** DMH Workforce Members shall be encouraged to make recommendations regarding changing DMH polices and procedures relating to PHI. Such recommendations should be submitted to the DMH Privacy Officer. The DMH Privacy Officer, or designee, shall review the recommendations that are received and take such actions as he or she considers appropriate. Efforts shall be made to keep a DMH Workforce Member apprised as to the outcome of his or her suggestion.

F. Mitigating Harmful Effects

DMH shall take all practicable steps to minimize any known harmful effects resulting from the unauthorized use or disclosure of PHI by a DMH Workforce Member and/or Business Associate and shall take steps to correct known instances of harm. Mitigation shall be determined on a case-by-case basis by the DMH Privacy Officer in consultation with legal counsel and other senior managers. Mitigation may include, but is not limited to, the following actions:

1. Retrieving the wrongfully disclosed information.

2. Notifying the individual who is the subject of the PHI, or his/her Personal Representative (PR), immediately of the wrongful disclosure. See Chapter 12, Right to an Audit Trail of Certain Disclosures of Protected Health Information.

3. Taking operational and procedural corrective measures to remedy the violation.

4. Taking action to discipline DMH Workforce Members as is necessary, up to and including termination.

5. Addressing problems with Business Associates once DMH is aware of a breach of privacy.

6. Incorporating mitigation solutions into DMH privacy policies and procedures.

G. Sanctions

DMH must have in place, apply and document application of appropriate sanctions against DMH Workforce Members who fail to comply with DMH policies and procedures relating to PHI.

1. **General.** DMH Workforce Members who violate DMH policies and procedures will be subject to appropriate disciplinary action, up to and including termination of employment. Not only is violation of DMH policies and procedures grounds for disciplinary action, but violations related to unauthorized use and disclosure of PHI may subject the DMH Workforce Member and DMH to civil and criminal penalties, including significant monetary costs and incarceration.

2. **Documentation.** If any DMH Workforce Member is sanctioned for the wrongful use or disclosure of PHI or for violating any other DMH policy or procedure relating to PHI, the violation and the sanction imposed shall be recorded in his or her personnel record. Upon request, the applicable Human Resources Office shall be able to provide the DMH Privacy Officer with a report of all sanctions relating to the infraction of DMH privacy policies and procedures that have been imposed during the six year period immediately preceding the request.

3. **Exceptions.** Sanctions shall not be applied to disclosures of PHI by DMH Workforce Members who are whistleblowers or crime victims if the following conditions are met:

    a. **Disclosure by Whistleblowers**:

        i. The DMH Workforce Member is acting in good faith and on the belief that DMH has engaged in conduct that is unlawful or otherwise violates professional or clinical standards or that the care, services and conditions provided by DMH potentially endangers a DMH service recipient, DMH Workforce Member or a member of the general public.

        ii. The disclosure is made to:

            - a federal or state Health Oversight Agency or Public Health Authority authorized by law to oversee the relevant conduct or conditions of DMH;
            - an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by DMH; or
            - an attorney retained by or on behalf of the DMH Workforce Member or Business Associate for the purpose of determining legal options regarding disclosure conduct.

        iii. The disclosing of PHI was necessary to report the "unlawful conduct" of DMH (e.g., the use of de-identified and/or a coding

system was not practical) and only that amount of PHI that was necessary to report the "unlawful act" was used to protect the privacy of the subject of the PHI.

b. **Disclosure by Crime Victims.** The DMH Workforce Member is the victim of a criminal act and discloses PHI to a law enforcement official about the suspected perpetrator of the criminal act and the disclosed PHI is limited to what is necessary for identification and location purposes.

H. Refraining From Intimidation or Retaliatory Acts

No DMH office, program, facility or DMH Workforce Member shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any:

1. individual, or his/her PR, if any, for exercising of his/her privacy rights;

2. person, including a DMH Workforce Member for filing in good faith a privacy complaint or non-compliance report with DMH or the U.S. Department of Health and Human Services, or for participating in a privacy related investigation, compliance review, proceeding or hearing;

3. DMH Workforce Member for helping an individual or his or her PR, if any, to exercise their privacy rights or to file a complaint or participate in a privacy related investigation; or

4. person opposing any act or practice alleged to be unlawful under state or federal law; provided the person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI.

I. Cannot Require the Waiver of Privacy Rights

No DMH office, program, facility or DMH Workforce Member shall require individuals to waive any of their privacy rights as a condition of treatment or eligibility for services. Privacy rights include the right to access records; the right to request amendments; the right to request restriction on the use or disclosure of PHI, the right to request confidential communications, and the right to an accounting of disclosures, as those rights are set forth in this Privacy Handbook.

III. LEGAL REFERENCE

HIPAA
45 CFR 164.530
45 CFR 164.502(j)